Vysoká škola báňská – Technická univerzita Ostrava

Fakulta metalurgie a materiálového inženýrství

Katedra automatizace a počítačové techniky v metalurgii

BAKALÁŘSKÁ PRÁCE

Architektura a implementace zabezpečení bezdrátových sítí

2010 **František DOLÁK**

VŠB - Technická univerzita Ostrava
Fakulta metalurgie a materiálového inženýrství
Katedra automatizace a počítačové techniky v metalurgii

Zadání bakalářské práce

Student: **František Dolák**

Studijní program: B3922 Ekonomika a řízení průmyslových systémů

Studijní obor: 3902R040 Automatizace a počítačová technika v průmyslu

Téma: Architektura a implementace zabezpečení bezdrátových sítí
Architecture and implementation of wireless networks security

Zásady pro vypracování:

1. Obecné technologie bezdrátového zabezpečení.
2. Návrh infrastruktury PKI.
3. Implementace zabezpečení 802.11x.
4. Zabezpečení klientských stanic.

Seznam doporučené odborné literatury:

1. BÁRTA, J. Úvod do počítačových sítí. Kopp: České Budějovice, 1995
2. SCHATT, S. Počítačové sítě LAN od A do Z. Grada: Praha, 1994
3. PENIAK, P., KALLAY, F. Počítačové sítě a jejich aplikace. Praha: Grada Publishing, 1999
4. JANČÍKOVÁ, Z. Základy počítačových sítí. Skripta, VŠB – TUO, Ostrava, 2007

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **prof. Ing. Zora Jančíková, CSc.**

Konzultant bakalářské práce: Ing. Robert Frischer

Datum zadání: 30.11.2009
Datum odevzdání: 21.05.2010

VYSOKÁ ŠKOLA BÁŇSKÁ - TECHNICKÁ UNIVERZITA Fakulta metalurgie a mat. inženýrství 1 OSTRAVA

prof. Ing. Milan Vrožina, CSc.
vedoucí katedry

prof. Ing. Ľudovít Dobrovský, CSc.,Dr.h.c.
děkan fakulty

Zásady pro vypracování bakalářské práce

I.

Bakalářskou prací (dále jen BP) se ověřují vědomosti a dovednosti, které student získal během studia, a jeho schopnosti využívat je při řešení teoretických i praktických problémů.

II.

Uspořádání bakalářské práce:

1. Titulní list + zásady pro vypracování BP
2. Prohlášení + místopřísežné prohlášení
3. Abstrakt + klíčová slova česky a anglicky
4. Obsah BP
5. Textová část BP
6. Seznam použité literatury
7. Přílohy

ad 1) Titulním listem je originál zadání BP, který student obdrží na své oborové katedře. Za titulním listem následují tyto „Zásady pro vypracování bakalářské práce".

ad 2) Prohlášení + místopřísežné prohlášení napsané na zvláštním listě (student jej obdrží na své oborové katedře) a vlastnoručně podepsané studentem s uvedením data odevzdání BP. *V případě, že BP vychází ze spolupráce s jinými právnickými a fyzickými osobami a obsahuje citlivé údaje, je na zvláštním listě vloženo prohlášení spolupracující právnické nebo fyzické osoby o souhlasu se zveřejněním BP.*

ad 3) Abstrakt a klíčová slova jsou uvedena na zvláštním listě česky a anglicky v rozsahu max. 1 strany pro obě jazykové verze.

ad 4) Obsah BP se uvádí na zvláštním listě. Zahrnuje názvy všech očíslovaných kapitol, podkapitol a statí textové části BP, odkaz na seznam příloh a seznam použité literatury, s uvedením příslušné stránky. Předpokládá se desetinné číslování.

ad 5)

Textová část BP obvykle zahrnuje:

- Úvod, obsahující charakteristiku řešeného problému a cíle jeho řešení v souladu se zadáním BP;
- Vlastní rozpracování BP (včetně obrázků, tabulek, výpočtů) s dílčími závěry, vhodně členěné do kapitol a podkapitol podle povahy problému;
- Závěr, obsahující celkové hodnocení výsledků BP z hlediska stanoveného zadání.

BP nemusí obsahovat experimentální (aplikační) část.

BP bude zpracována v rozsahu min. 25 stran (včetně obsahu a seznamu použité literatury).

Text musí být napsán vhodným textovým editorem počítače po jedné straně bílého nelesklého papíru formátu A4 při respektování následující **doporučené** úpravy - písmo Times New Roman (nebo podobné) 12b; řádkování 1,5; okraje – horní, dolní – 2,5 cm, levý – 3 cm, pravý 2 cm. Fotografie, schémata, obrázky, tabulky musí být očíslovány a musí na ně být v textu poukázáno. Budou zařazeny průběžně v textu, pouze je-li to nezbytně nutné, jako přílohy (viz ad 7).

Odborná terminologie práce musí odpovídat platným normám. Všechny výpočty musí být přehledně uspořádány tak, aby každý odborník byl schopen přezkoušet jejich správnost. U

vzorců, údajů a hodnot převzatých z odborné literatury nebo z praxe musí být uveden jejich pramen - u literatury citován číselným odkazem (v hranatých závorkách) na seznam použité literatury.
Nedostatky ve způsobu vyjadřování, nedostatky gramatické, neopravené chyby v textu mohou snížit klasifikaci práce.

ad 6) BP bude obsahovat alespoň 10 literárních odkazů, z toho nejméně 3 v některém ze světových jazyků.
Seznam použité literatury se píše na zvláštním listě. **Citaci literatury je nutno uvádět důsledně v souladu s ČSN ISO 690.** Na práce uvedené v seznamu použité literatury musí být uveden odkaz v textu BP.

ad 7) Přílohy budou obsahovat jen ty části (speciální výpočty, zdrojové texty programů aj.), které nelze vhodně včlenit do vlastní textové části, např. z důvodu ztráty srozumitelnosti.

III.

Bakalářskou práci student odevzdá ve dvou knihařsky svázaných vyhotoveních, pokud katedra garantující studijní obor neurčí jiný počet. Vnější desky budou označeny takto:

nahoře: *Vysoká škola báňská - Technická univerzita Ostrava*
Fakulta metalurgie a materiálového inženýrství
Katedra . . . . . .

uprostřed: *BAKALÁŘSKÁ PRÁCE*

dole: *Rok* *Jméno a příjmení*

Kromě těchto dvou knihařsky svázaných výtisků odevzdá student kompletní práci také v elektronické formě do IS EDISON včetně abstraktu a klíčových slov v češtině a angličtině.

IV.

Bakalářská práce, která neodpovídá těmto zásadám, nemůže být přijata k obhajobě. Tyto zásady jsou závazné pro studenty všech studijních programů a forem bakalářského studia fakulty metalurgie a materiálového inženýrství Vysoké školy báňské – Technické univerzity Ostrava od akademického roku 2009/2010.

Ostrava 30. 11. 2009

Prof. Ing. Ludovít Dobrovský, CSc., Dr.h.c.
děkan fakulty metalurgie a materiálového inženýrství
VŠB-TU Ostrava

P R O H L Á Š E N Í

Prohlašuji, že

- jsem byl(a) seznámen(a) s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. - autorský zákon, zejména §35 - užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního (§60 - školní dílo);

- beru na vědomí, že Vysoká škola báňská - Technická univerzita Ostrava (dále jen VŠB - TUO) má právo nevýdělečně ke své vnitřní potřebě bakalářskou práci užít (§35 odst. 3);

- souhlasím s tím, že bakalářská práce bude archivována v elektronické formě v databázi Ústřední knihovny VŠB - TUO a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO;

- bylo sjednáno, že s VŠB - TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu §12 odst. 4 autorského zákona;

- bylo sjednáno, že užít své dílo - bakalářskou práci nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB - TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB - TUO na vytvoření díla vynaloženy (až do jejich skutečné výše);

- beru na vědomí, že odevzdáním své bakalářské práce souhlasím s jejím zveřejněním podle zákona č. 111/1998Sb., o vysokých školách a o změně a doplnění dalších zákonů (Zákon o vysokých školách) bez ohledu na výsledek její obhajoby.

Místopřísežně prohlašuji, že jsem celou bakalářskou práci vypracoval(a) samostatně.

V Ostravě 21. 5. 2010

František Dolák

.....

podpis (jméno a příjmení studenta)

P o d ě k o v á n í

Děkuji prof. Ing. Z. Jančíkové, CSc. a Ing. R. Frischerovi za odborné vedení bakalářské práce, za připomínky a konzultace.

Abstrakt

Bakalářská práce je zaměřena na problematiku zabezpečení bezdrátové sítě v produkčním prostředí.

První kapitola se zabývá obecnou problematikou zabezpečení, typy, jejich volbou i možnostmi zneužití bezdrátových sítí.

Hlavním tématem bakalářské práce je návrh síťové infrastruktury a jejích podpůrných služeb, vybudování infrastruktury PKI (Public Key Infrastructure) a implementace ověřování klientů za podpory standardu 802.11i a technologií společnosti Microsoft, kteří nejsou součástí domény.

V závěru práce jsou uvedeny další problémy, které narušují zdárný chod infrastruktury a záležitosti, na které musí být v produkčním prostředí pamatováno.

Abstract

Bachelor's thesis is focused on wireless security in enterprise environment. The first chapter deals with the general issue of security, their types and choices and the possibility of wireless network abuse.

The main topic of this work is to design network infrastructure and related services, build Public Key Infrastructure PKI, and implement and validate non-domain clients all with the support of 802.11i standard Microsoft technologies. At the same time, publishing of client certificates will be fully authorized by a Certification Authority.

At the end of our work there are shown other problems and matters that interfere with the successful operation of infrastructure and must be remembered of in a production environment.

OBSAH

Úvod

Všudypřítomnost bezdrátových sítí je v dnešním světě už prakticky samozřejmostí.Když pomineme domácnosti a jednotlivce, stále více společností využívá výhody „volného“ pohybu zařízení oproti fyzickému připojení.Bezdrátové sítě dnes nabízejí kavárny, letiště a další místa, kde si lze přečíst elektronickou poštu, internetový tisk nebo například využívat služby e-banking.

Bohužel, navzdory snadnému užití bezdrátových sítí a jejich masivnímu rozsahu, roste prudce otázka bezpečnosti.Je až zarážející, jak někteří poskytovatelé internetových služeb staví svoje rozsáhlé sítě s primárním zabezpečením typu filtrace MAC adres a seznamu přístupových oprávnění ACLs, jež jsou se vzrůstajícím prostředím neudržitelné a které považuji spíše jako sekundární bezpečnostní prvky.

Na proti tomu, IEEE 802.1x je technologií, která zajišťuje téměř neomezenou škálovatelnost s minimálními nároky na administraci a nejsilnější možnou ochranou bezdrátových produkčních prostředí.

V následujících částech Vás nejprve seznámím s celou řadou možností zabezpečení bezdrátových sítí, uvedu některá jejich hlavní úskalí a dále se budu věnovat konfiguraci síťové infrastruktury 802.1x. Provedu Vás problematikou nastavení infrastruktury veřejných klíčů (PKI) a v závěru dokončíme implementaci zabezpečením autentizace bezdrátových klientů, kteří nejsou součástí domény.

1. OBECNÉ TECHNOLOGIE BEZDRÁTOVÉHO ZABEZPEČENÍ

V roce 1997 byla přijata specifikace 802.11, která podporovala protokol, který zahrnoval první a druhou vrstvu modelu OSI. V roce 1999 byly uvedeny doplňky v podobě 802.11a a 802.11b.V roce 2003 přibyl doplněk 802.11g.

Protokol WEP

Protokol WEP má mnoho zranitelných míst, které byly zdokumentovány a které omezují schopnost ochrany přenášených dat. Problém je v použití šifrovacího mechanismu RC4[1], který protokol WEP používá, respektive v jeho použití. Hlavním problémem je chyba v implementaci inicializačního vektoru, jelikož v silném provozu se může opakovaně používat stejná hodnota klíče z důvodu rychlého vyčerpání 24bitového klíče. Řešením problému je zvětšení inicializačního vektoru a v zabránění opakovaného užití stejné hodnoty. Další problém je v generátoru 40 bitového klíče, který při dnešní výpočetní síle je prolomen během několika sekund. Poslední problém, o kterém se zmíním, je v mechanismu generování klíče, který lze zneužít například programem AirSnort[2], kdy lze na sítích s velkým provozem odposlouchávat pakety a následně dešifrovat 64 a 128 bitové klíče za velmi krátkou dobu.

Protokol WPA

V roce 2002 tento protokol vydala Wi-Fi aliance. V této době byly hotové pouze určité části specifikace 802.11i, jako 802.1x a TKIP. Tyto technologie přinesly řešení řady slabin protokolu WEP a 802.11, zejména zvýšením inicializačního vektoru na 48 bitů a změnou kontroly integrity pomocí funkce Michael a funkcí mixování klíče pro každý paket.

Protokol WPA2

Základem protokolu WPA2 je specifikace 802.11i, kde primární komponentou je šifra AES, která nahrazuje RC4.Stejně jako RC4 je AES šifra se symetrickým klíčem. Na rozdíl od RC4, která šifruje lineárně každý bajt funkcí XOR s náhodnou sekvencí, AES pracuje s bloky velikosti 128 bitů.

Protokol 802.1x

Tento protokol pracuje na principu autentizace na portech. V tomto kontextu myslím port jako součást první síťové vrstvy, tj. fyzické porty na přepínači. V principu lze chápat každého bezdrátového klienta jako virtuální metalické připojení. Protokol 802.1x blokuje veškerý provoz na daném portu do té doby, než se klient autentizuje specifickými údaji, které jsou uloženy na back-end serveru, obvykle server Radius[5].

802.1x má tři hlavní komponenty:

- Žadatele, což je klientské pc
- Autentizátora, což je zařízení "uprostřed", typicky AP
- Autentizační server, obvykle Radius

Protokol EAP

Tento protokol byl primárně vytvořen pro protokol PPP, který se používal pro DSL modemy apod. Bohužel tento protokol čelí jistým omezením v podobě autentizace, která umožňuje pouze autentizaci na bázi uživatelského jména a hesla.EAP přišel s rozšířením v podobě autentizačních modulů, díky kterým lze k autentizaci užít certifikáty,PKI, čipové katry, biometriku apod.

EAP a jeho autentizační metody

802.1x a EAP jsou pouze základnou pro provozování zabezpečené autentizační výměny.

Existuje řada autentizačních metod. Obvykle se liší obtížností implementace, bezpečnostní úrovní případně kompatibilitou firem (CISCO, Certicom, Microsoft)a v neposlední řadě i cenou.

Z důvodu implementace zabezpečení bezdrátové sítě pomocí technologií Microsoft, uvedu zde pouze dvě metody:

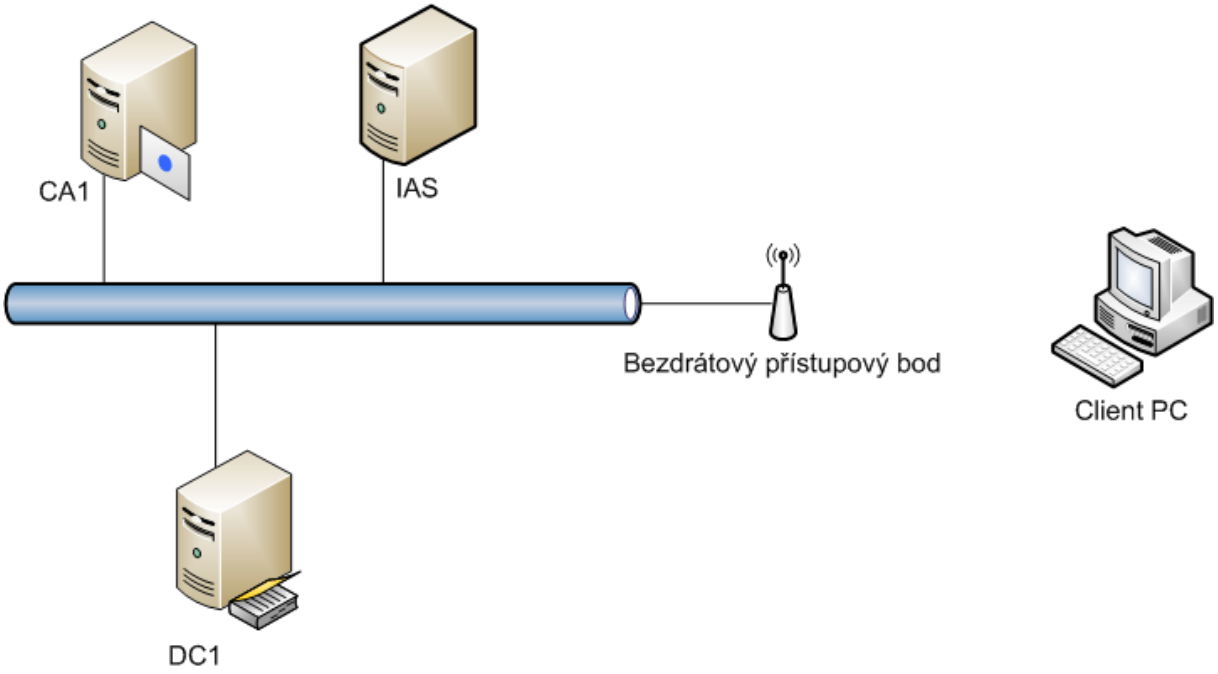
- PEAP
- TLS

PEAP neboli Protected-EAP vyžaduje certifikát a to pouze na straně serveru.Autentizace klientů probíhá zabezpečeně, kdy prostřednictvím certifikátu dojde k autentizaci serveru a následně použití jiné ověřovací metody, např. zadání uživatelského jména a hesla.

TLS- je nejsilnější možné zabezpečení, naopak implementace je nejobtížnější. Nutností je mít certifikáty jak na straně serveru, tak i na klientské stanici. Z tohoto je zřejmé, že je třeba vybudovat infrastrukturu PKI.TLS poskytuje vzájemnou autentizaci i dynamickou obnovu wepových klíčů.

Jak už jsem uvedl dříve, dále se budu zabývat postupem implementace 802.1x, EAP-TLS a šifrováním AES za použití technologií Microsoft.

2. NÁVRH INFRASTRUKTURY PKI



2.1.INSTALACE DOMÉNOVÉHO ŘADIČE (DC1)

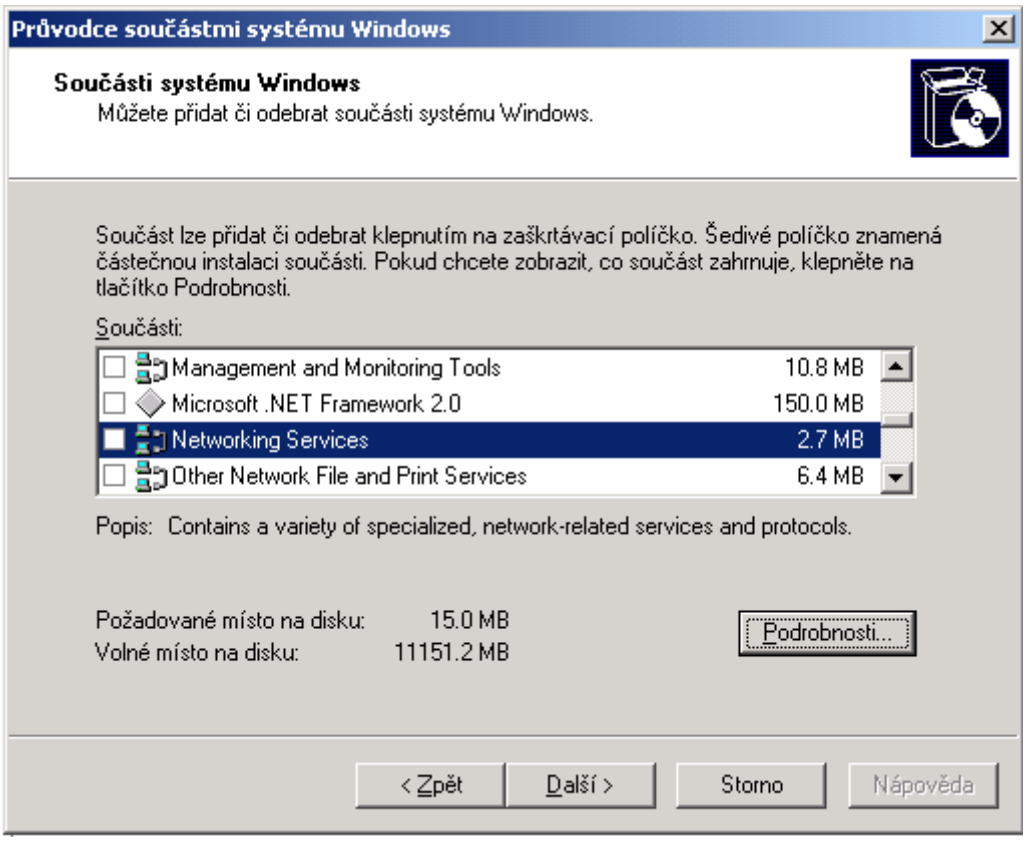
1. Nainstalujte Windows server 2003 R2 Enterprise Edition na server (stand- alone)
2. Nastavte síťovou adresu TCP/IP protokolu na 192.168.20.2 a masku podsítě na 255.255.255.0, server DNS nastavte na 192.168.20.2[6]

Pozn.: Adresu serveru DNS lze nastavit i po instalaci a konfiguraci služby DNS

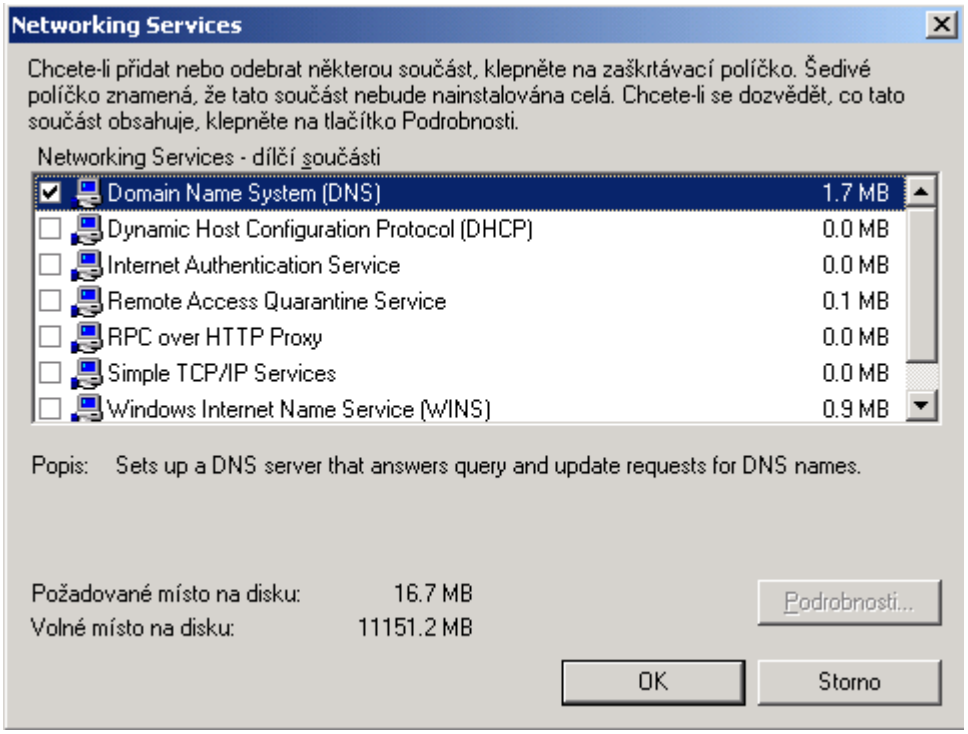
2.1.1. Instalace služby DNS

1. Přihlaste se k serveru **Dc1** jako **správce**
2. V **Nabídce Start** přejděte na **Ovládací panely** a dále klikněte na **Přidat nebo odebrat programy**.
3. V levém menu klikněte na **Přidat nebo odebrat součásti systému.**

4. V průvodci součástmi vyberte položku **Networking services** (síťové služby) a dále na **Podrobnosti**, (viz obr1.).
5. V okně **Networking services** zatrhněte položku **Domain Name System (DNS)** a klikněte na tlačítko **OK**. Po vyzvání vložte instalační disk Windows Serveru do jednotky cd-rom a stiskněte **OK**. Po úspěšné instalaci klikněte na **Dokončit**.



Obr. 1



Obr. 2

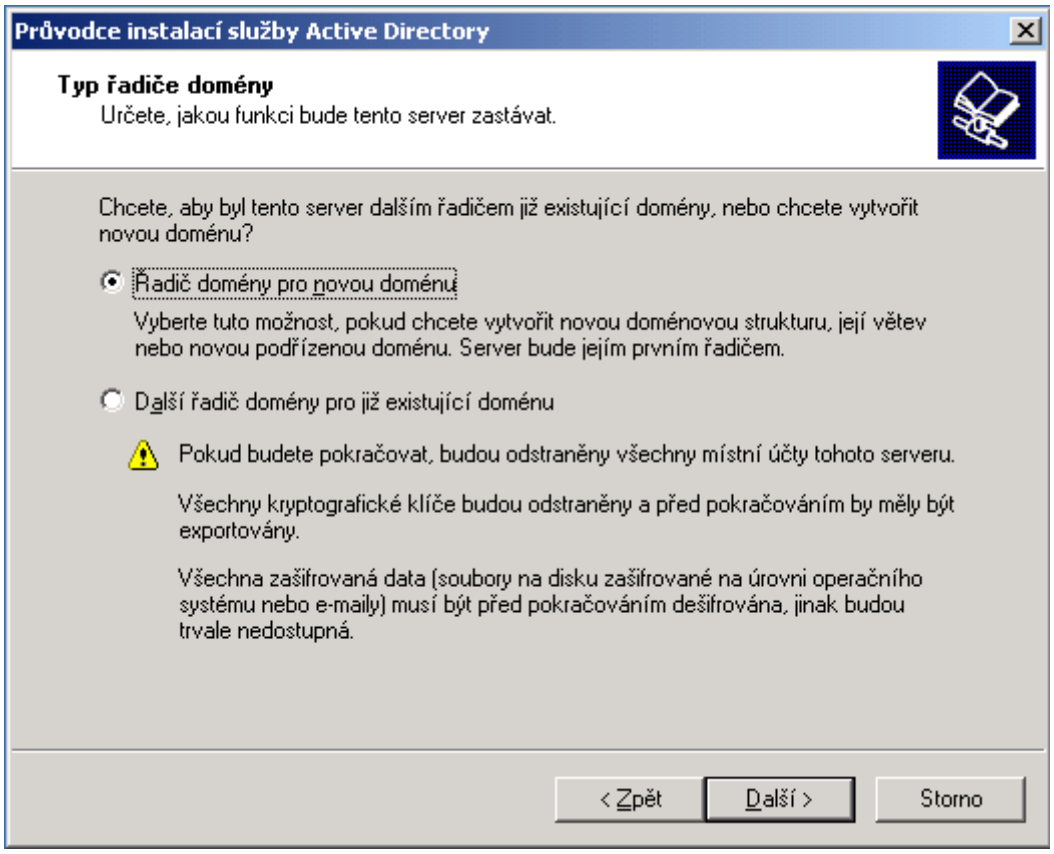
2.1.2. Konfigurace služby DNS

1. V **Nabídce Start** přejděte do položky **Nástroje pro správu** a klikněte na položku **DNS**.
2. V levém okně rozbalte strom DC1 a pravým tlačítkem klikněte na položku **Zóny dopředného vyhledávání** a vyberte **Nová zóna**. Po zobrazení průvodce klepněte na tlačítko **Další**.
3. V dialogovém okně **Typ zóny** zatrhněte **Primární zóna** a pokračujte tlačítkem **Další**.
4. Jako **název zóny** uveďte název vaší organizace, např. **maxdat.cz** a klikněte na tlačítko **Další**.
5. V dialogovém okně **Soubor zóny** překontrolujte, že je zaškrtnuta volba **Vytvořit nový soubor s následujícím názvem** a že text v poli obsahuje **maxdat.cz.dns**. Dále pak klepněte na **Další**.
6. V okně **Dynamické aktualizace** zvolte volbu **Povolit nezabezpečené a zabezpečené dynamické aktualizace** a klepněte na **Další**. Na závěr klepněte na tlačítko **Dokončit**.
7. V poli **Název počítače** ověřte, že je zadaný název **dc1** a poté pokračujte tlačítkem **Další**.

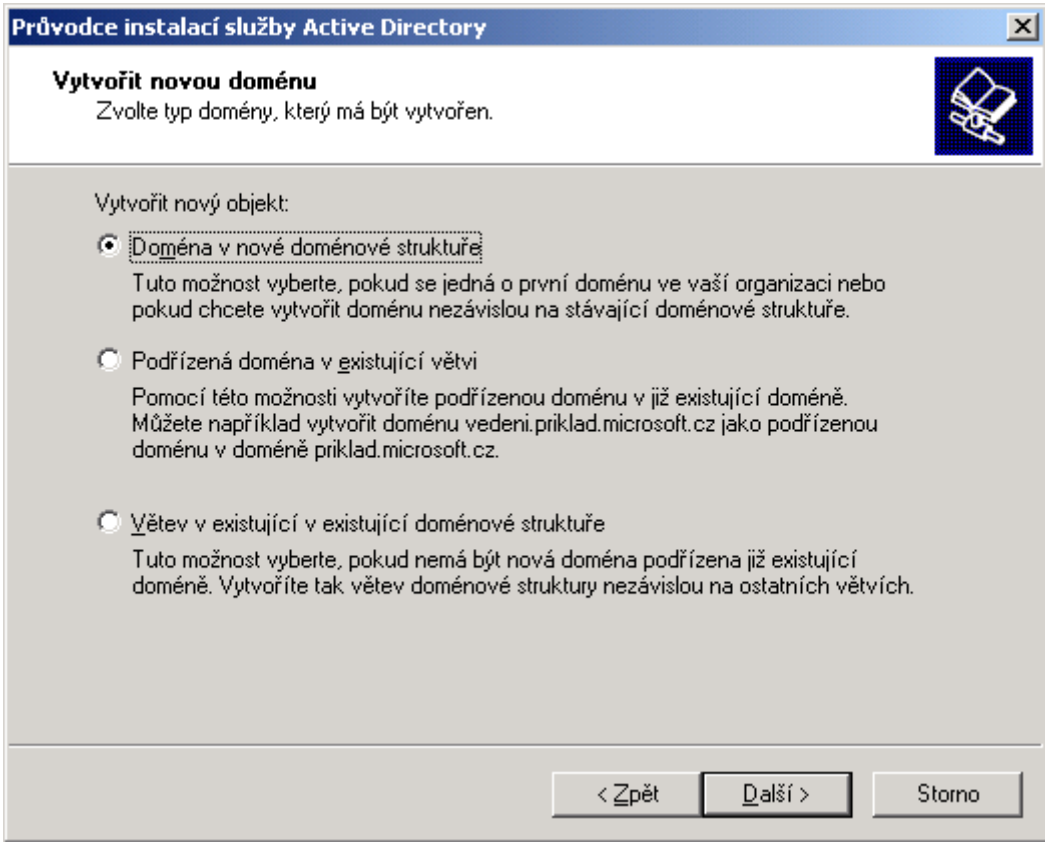
8. V poli **Primární přípona DNS tohoto počítače** zadejte **maxdat.cz** a klikněte na tlačítko **Další** a **OK**.
9. Po výzvě k restartu počítač **restartujte**.

2.1.3. Instalace doménového řadiče

1. V **Nabídce Start** klikněte na **Spustit** a do dialogového okna zadejte příkaz **dcpromo** a klikněte na **OK**. Po zobrazení průvodce instalací služby Active directory klepněte na **Další** a **Další**.[4]
2. V dialogovém okně **Typ řadiče domény** zvolte **Řadič domény pro novou doménu** a pokračujte tlačítkem **Další**.(viz obr.3)
3. V okně **Vytvořit novou doménu** zvolte **Doména v nové doménové struktuře** a klikněte na **Další**.(viz obr.4)

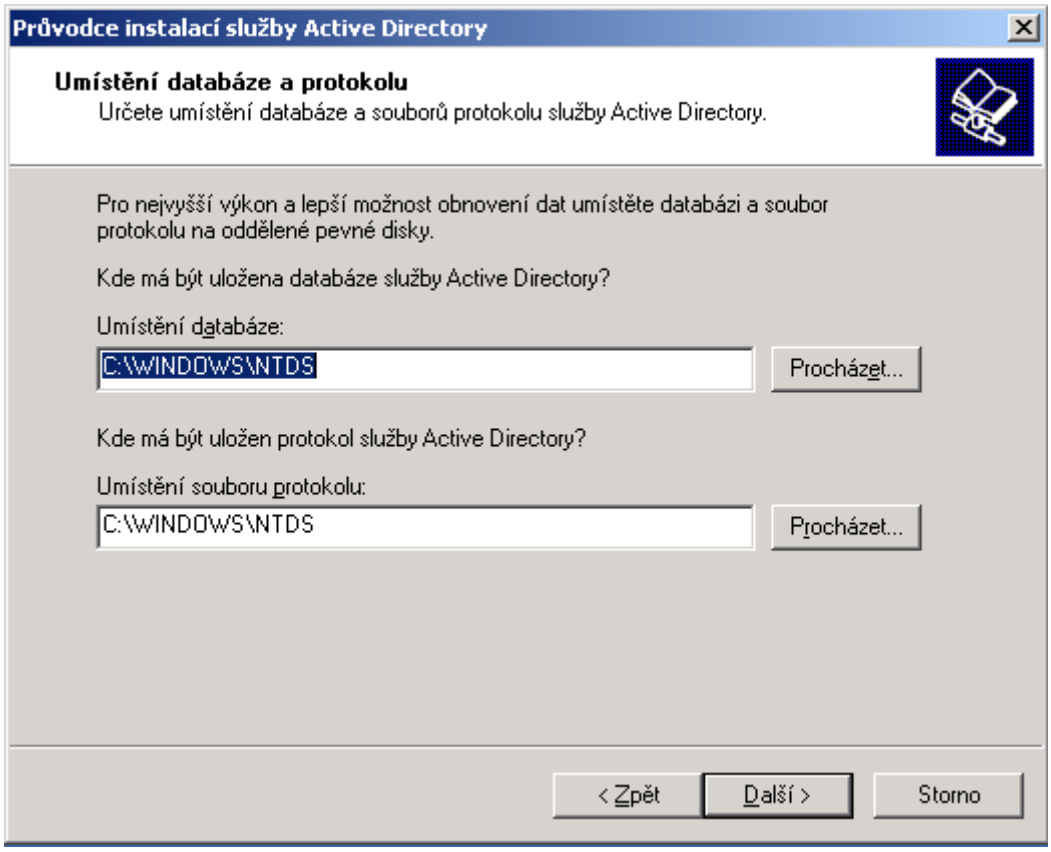


Obr. 3



Obr. 4

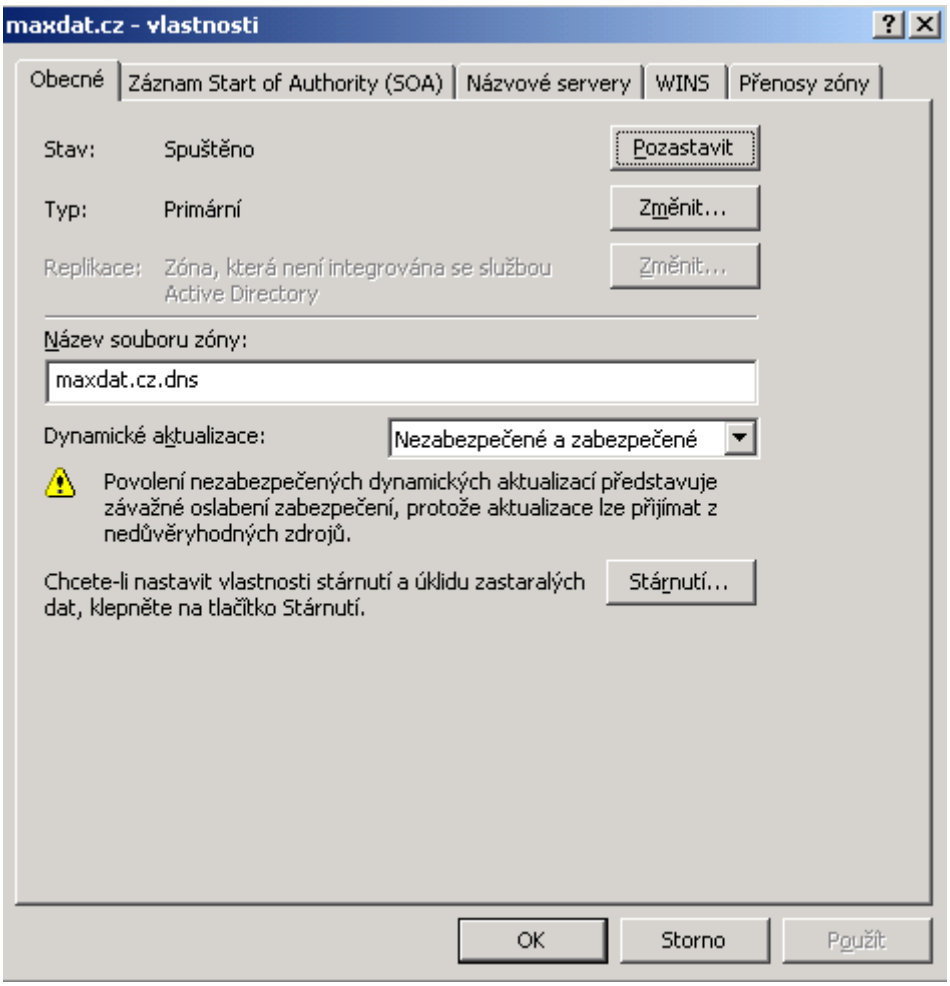
4. V dialogovém okně **Název nové domény** zadejte do pole **maxdat.cz** a klikněte na **Další**.
5. Ponechte v poli **Název domény pro rozhraní NetBIOS** výchozí položku **MAXDAT** a dejte **Další**.
6. Umístění databáze a protokolu nechte ve výchozím nastavení a klikněte na tlačítko **Další**. (viz obr.5).
7. V dialogovém okně **Sdílený systémový svazek** ponechte **výchozí nastavení** a klikněte na **Další**.
8. Prohlédněte si diagnostické informace a dejte **Další**.
9. V dialogovém okně **Oprávnění** vyberte položku **Oprávnění kompatibilní pouze s operačními systémy řady Windows 2000 Server nebo Windows Server 2003** a klikněte na **Další**.
10. Zadejte heslo pro režim obnovení adresářových služeb s následným potvrzením a pokračujte tlačítkem **Další**.
11. V okně **Souhrn** zkontrolujte nastavení, a pokud vše souhlasí, klepněte na **Další**.
12. Po dokončení instalace řadiče je nutné server **restartovat**.



Obr. 5

2.1.4. Konfigurace DNS na doménovém řadiči

1. Přihlaste se k **Dc1** jako **správci** a spusťte **konzolu DNS**.
2. **Rozbalte** strom DC1 a následně **Zóny dopředného vyhledávání** v levém menu, klikněte pravým tlačítkem na název domény **maxdat.cz** a zvolte **Vlastnosti**.(viz obr.6).



Obr. 6

3. Na kartě **Obecné** klikněte na tlačítko **Změnit** a v dialogovém okně **Změnit typ zóny** vyberte **Primární zóna** a zatrhněte volbu **Uložit zónu do adresáře Active Directory (dostupné pouze pokud je server DNS řadičem domény).** Poté klepněte na **OK**.
4. Po výzvě zdali chcete, aby se tato zóna stala integrovanou se službou Active Directory, klepněte na **Ano**.
5. Na kartě **Obecné** v poli **Dynamické aktualizace** zvolte **Pouze zabezpečené** a dejte **OK.**

2.1.5. Povýšení úrovně funkčnosti domény

1. V **Nabídce Start** v **Nástrojích pro správu** zvolte **Uživatelé a počítače služby Active Directory.**
2. V levém menu klikněte na název domény maxdat.cz pravým tlačítkem a zvolte **Zvýšit úroveň funkčnosti domény.**
3. V poli **Vyberte dostupnou úroveň funkčnosti domény**, zvolte **Windows Server 2003** a klikněte na tlačítko **Zvýšit.**
4. Po zobrazení varovné zprávy, klikněte na tlačítko **OK.**

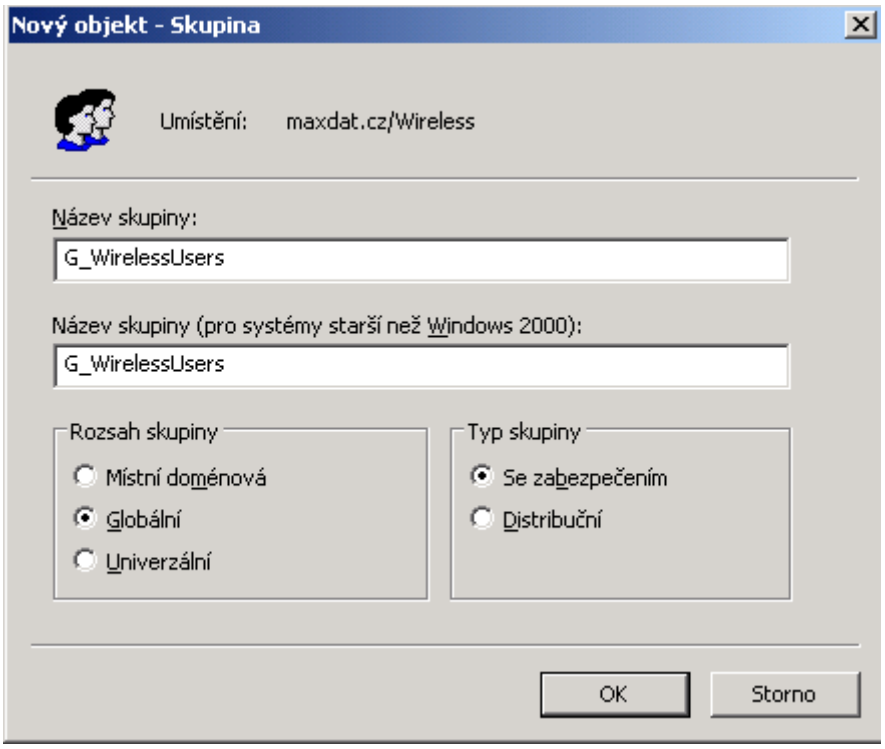
2.1.6. Instalace služby DHCP

1. V **Nabídce Start** -> **Ovládací panely**->**Přidat nebo odebrat programy** -> **Přidat nebo odebrat součásti systému** rozbalte volbu **Síťové služby (Networking services)** a zaškrtněte volbu **Pomocí protokolu DHCP (Dynamic Host Configuration Protokol)** a stiskněte **OK.** Poté pokračujte tlačítkem **Další.**
2. Po instalaci služby klikněte na tlačítko **Dokončit.**
3. V **Nabídce Start** v **Nástrojích pro správu** zvolte **konzolu DHCP**, klikněte pravým tlačítkem na název serveru dc1.maxdat.cz a dejte **Nový obor**. Po spuštění průvodce klikněte na **Další.**
4. V průvodci vytvořením oboru v poli **Název** zadejte **název** (např. Centrála) , případně **popis** a klikněte na **Další.**
5. V okně **Rozsah adres IP** zadejte do pole **Počáteční adresa** IP 192.168.20.20 a do pole **Koncová adresa IP** 192.168.20.254. **Maska podsítě** bude 255.255.255.0 a klikněte na **Další.**
6. V dialogovém okně **Přidat vyloučení** nechejte ve **výchozím** nastavení a dejte **Další.**
7. **Dobu trvání** ponechte **výchozí** a pokračujte stiskem tlačítka **Další.**
8. V dialogovém okně **Konfigurovat možnosti serveru DHCP** zvolte **Ne, změním tyto možnosti později** a klepněte na **Další**. Poté dejte tlačítko **Dokončit.**
9. Pravým tlačítkem klikněte na **Možnosti oboru** a zvolte **Konfigurovat možnosti.**

10. Na kartě **Obecné** zatrhněte volbu **006 Servery DNS** a do pole **Adresa IP** zadejte 192.168.20.2 a klikněte na **Přidat.** Pak pokračujte tlačítkem **OK.**
11. **V konzole DHCP** klikněte pravým tlačítkem na **Obor [192.168.20.0]Centrála** a zvolte **Aktivovat**.
12. Klikněte na název serveru dc1.maxdat.cz a v menu **Akce** zvolte **Ověřit.**

2.1.7. Vytvoření uživatelské skupiny a účtu pro bezdrátové klienty

1. V **Nabídce Start** v **Nástrojích pro správu** zvolte **Uživatelé a počítače služby Active Directory.**
2. Klikněte pravým tlačítkem na název domény maxdat.cz, najeďte do **Nová položka** a zvolte **Organizační jednotka.**
3. Zadejte název **Wireless** a stiskněte **OK.**
4. Nyní klikněte na nově vytvořenou jednotku **Wireless** v levém menu a opět pravým tlačítkem zvolte **Nová položka** a dejte **Skupina.**
5. Zadejte do pole **Název skupiny** G_WirelessUsers a stiskněte **OK.**(viz obr.7)



Obr. 7

6. Zadejte do pole **Název skupiny** G_WirelessUsers a stiskněte **OK.**
7. Opět klikněte na vytvořenou jednotku Wireless v levém menu a pravým tlačítkem zvolte **Nová položka** a klikněte na položku **Uživatel.**
8. Do pole **Jméno** a **Přihlašovací uživatelské jméno** zadejte **WirelessUser** a klepněte na **Další.**
9. Zadejte heslo pro daného uživatele, potvrďte ho opětovným zadáním a všechny volby ponechte **nezatrhlé.** Pak stiskněte **Další** a následně tlačítko **Dokončit.**
10. V konzole **Uživatelé a počítače služby Active Directory** klikneme na pravé straně na položku **WirelessUser** pravým tlačítkem a zvolíme **Vlastnosti.**
11. Na kartě **Telefonická připojení** v poli **Oprávnění ke vzdálenému přístupu (telefonní připojení neb VPN)** zvolíme volbu **Povolit přístup** a dáme **OK.**
12. V konzole **Uživatelé a počítače služby Active Directory** klikneme na pravé straně na položku **G_WirelessUsers** pravým tlačítkem a zvolíme **Vlastnosti.**
13. Přepneme se na kartu **Členové** a dáme **Přidat**. Do pole **Zadejte názvy objektů k výběru** napíšeme **WirelessUser** a klikneme na tlačítko **Kontrola názvů** a dáme **OK.**
14. Zavřeme dialogové okno stisknutím **OK.**

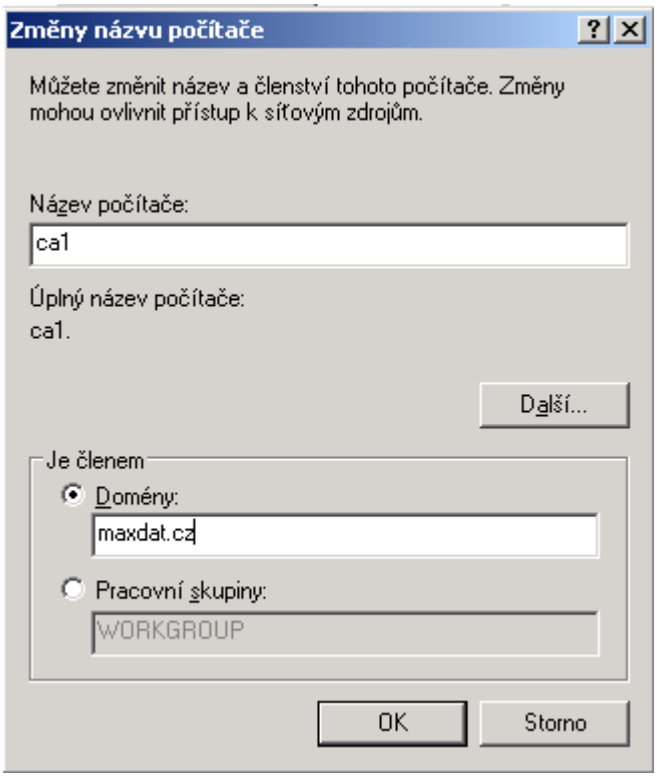
2.2.INSTALACE CERTIFIKAČNÍHO SERVERU (CA1)

1. Nainstalujte Windows server 2003 R2 Standard nebo Enterprise Edition na server (stand- alone)
2. Nastavte síťovou adresu TCP/IP protokolu na 192.168.20.3 a masku podsítě na 255.255.255.0, server DNS nastavte na 192.168.20.2

Pozn.: U tohoto typu prostředí nebudeme využívat autoenrolment technologii a automatické publikování certifikátů, proto lze užít i verzi Windows Server 2003 Standard!

2.2.1. Přidání serveru CA1 do doménového prostředí

1. Najeďte do **Nabídky Start**, **pravým** tlačítkem klikněte na položku **Tento počítač** a zvolte **Vlastnosti**.[11]
   V dialogovém okně **Vlastnosti systému** zvolte kartu **Název počítače** a dejte **Změnit.**
2. V poli **název počítače** ověřte, že název je **ca1.**(viz obr.8)
3. V poli **Je členem** vyberte volbu **Domény** a do jejího pole zadejte **maxdat.cz** a stiskněte **OK.**
4. Zadejte uživatelské jméno a heslo s oprávněním se připojit do domény. (Administrator) a dejte **OK.**
5. Po zobrazení dialogového okna Vítejte v doméně maxdat.cz klikněte na **OK** a **OK** a po výzvě **restartujte** server.



Obr. 8

2.2.2. Instalace IIS a certifikační autority

1. Přihlaste se k serveru **CA1** jako **správce** a jako **člen domény.**
2. V **Nabídce Start** přejděte na **Ovládací panely** a dále klikněte na **Přidat nebo odebrat programy**.
3. V levém menu klikněte na **Přidat nebo odebrat součásti systému.**
4. V průvodci součástmi vyberte položku **Aplikační server** (Application server) a klikněte na **Další.** Po vyzvání vložte instalační disk Windows Serveru do jednotky cd-rom a stiskněte **OK.** Po úspěšné instalaci klikněte na **Dokončit.**[8]
5. Opětovně klikněte na **Přidat nebo odebrat součásti systému** a v průvodci součástmi vyberte **Certifikační služba** (Certificate services) a stiskněte **Další.** Po přečtení výstrahy, že název serveru nelze po instalaci změnit, klikněte na **Ano** a stiskněte **Další.**
6. V dialogovém okně **Typ certifikačního úřadu** zvolte **Kořenový CU rozlehlé sítě** a pokračujte tlačítkem **Další.**

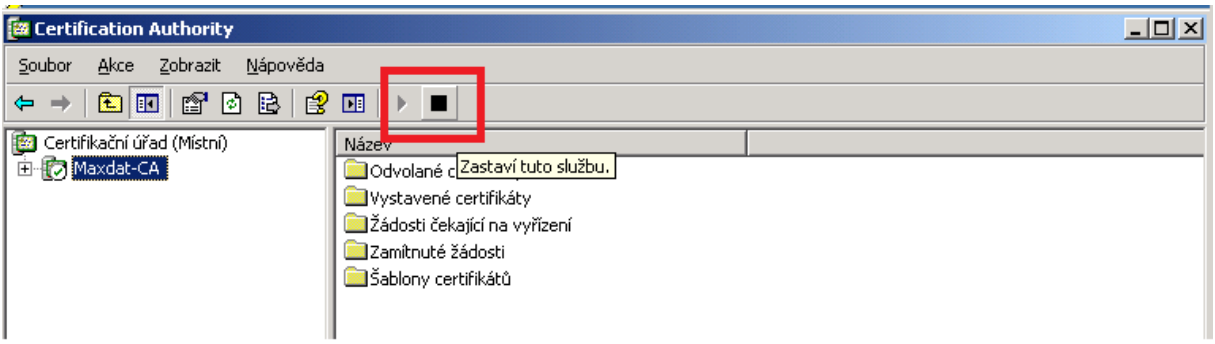
7. V okně **Identifikační informace certifikačního úřadu** v poli **Běžný název tohoto CÚ** zadejte Maxdat-CA a klikněte na **Další.**
8. V dialogovém okně **Nastavení certifikační databáze** ponechte **výchozí** nastavení a klepněte na **Další.**
9. Po varování o pozastavení IIS služby z důvodu instalace CÚ dejte **Ano** a před dokončením instalace dojde k dalšímu varování z hlediska bezpečnosti ASP, zvolte **Ano.** Instalaci dokončíte stisknutím klávesy **Dokončit.**

Pozn.: Při přihlašování k serveru dávejte pozor na pole **Přihlásit se k**, kde musí být vybrána položka Maxdat. Pokud se přihlásíte jako CA1 dojde k chybám ve spojení a certifikační autorita selže.

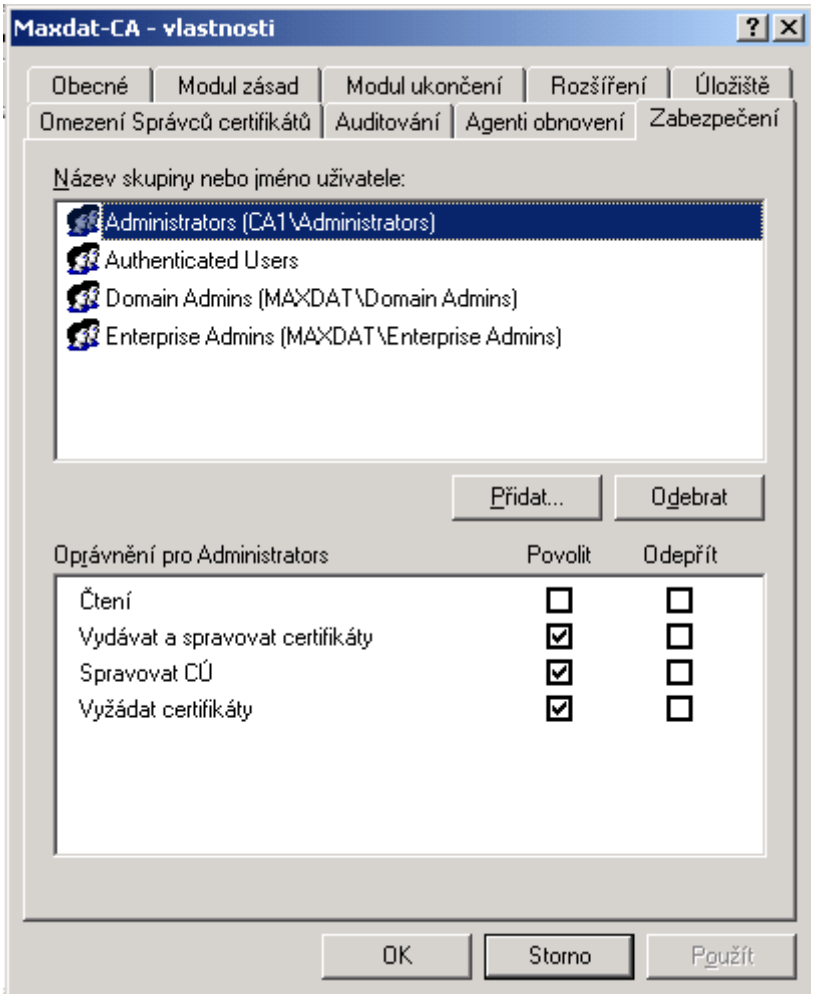
2.2.3. Konfigurace oprávnění a zákaz autoenrollmentu CA

1. V **Nabídce Start** v **Nástrojích pro správu** klepněte na **Certifikační úřad.**[14]
2. V levém menu konzoly klikněte **pravým** tlačítkem na Maxdat-CA a dejte **Vlastnosti.**
3. Na kartě **Zabezpečení** klepněte na **Administrators** a zaškrtněte položky **Vydávat** a **Spravovat** certifikáty, **Spravovat CÚ**, **Vyžádat certifikáty** a klikněte na **OK.**(viz obr.10)
4. Dále klepněte na kartu **Modul zásad** a dejte **Vlastnosti.**
5. Zvolte možnost **Nastavit stav žádosti o certifikát n**a **čekající na vyřízení, správce musí tento certifikát vystavit explicitně** a potvrďte nastavení tlačítkem **OK.**

Jak CA upozorňuje, je třeba restartovat službu certification sevices a to způsobem kliknutím na symboly Zastavit a Spustit službu viz následující obrázek menu.(viz obr.9)


Certification Authority
Soubor
Akce
Zobrazit
Nápověda
Certifikační úřad (Místní)
Maxdat-CA
Název
Zastaví tuto službu.
Vystavené certifikáty
Žádosti čekající na vyřízení
Zamítnuté žádosti
Šablony certifikátů

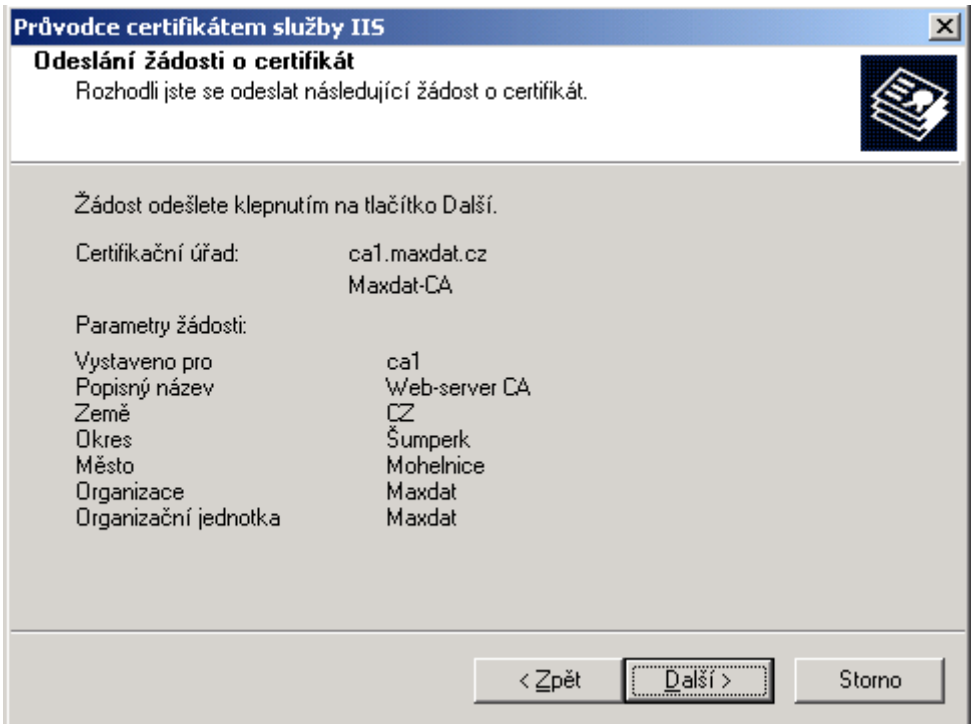
Obr. 9


Maxdat-CA - vlastnosti
Obecné
Modul zásad
Modul ukončení
Rozšíření
Úložiště
Omezení Správců certifikátů
Auditování
Agenti obnovení
Zabezpečení
Název skupiny nebo jméno uživatele:
Administrators (CA1\Administrators)
Authenticated Users
Domain Admins (MAXDAT\Domain Admins)
Enterprise Admins (MAXDAT\Enterprise Admins)
Přidat...
Odebrat
Oprávnění pro Administrators
Povolit
Odepřít
Čtení
Vydávat a spravovat certifikáty
Spravovat CÚ
Vyžádat certifikáty
OK
Storno
Použít

Obr. 10

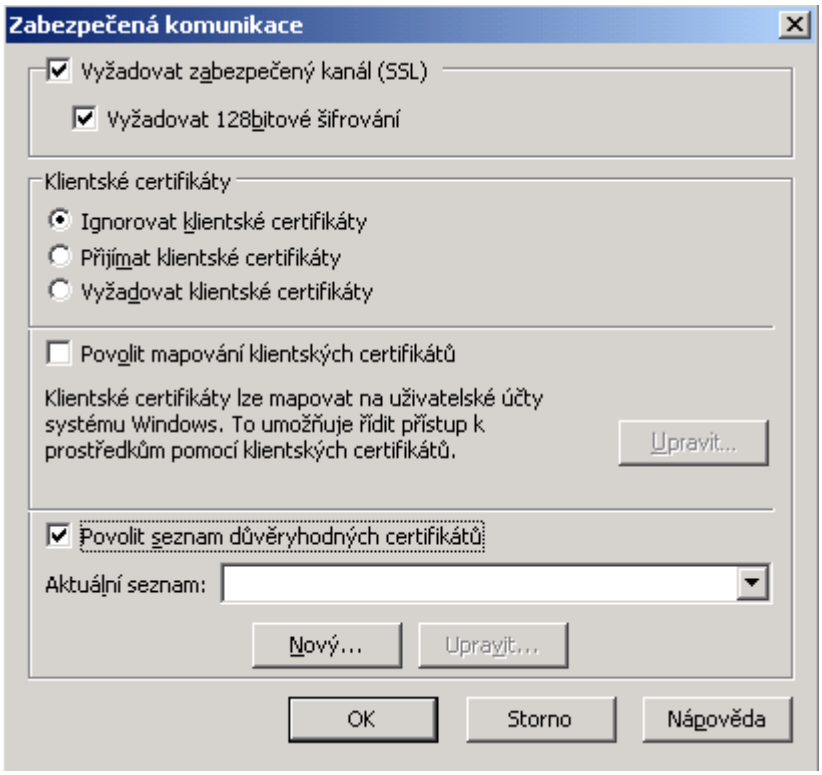
2.2.4. Posílení zabezpečení IIS na HTTPS

1. V **Nabídce Start**-> **Nástroje pro správu** zvolte **Správa internetové informační služby.**[13]
2. Rozbalte složku **Webové servery**, pravým tlačítkem klikněte na **Default Web Site** a zvolte **Vlastnosti.**
3. Vyberte kartu **Zabezpečení adresáře** a v poli **Zabezpečená komunikace** klepněte na tlačítko **Certifikát serveru.** Po přečtení průvodce klikněte na **Další.**
4. V dialogovém okně **Certifikát serveru** zvolte **Vytvořit nový certifikát** a pokračujte stisknutím tlačítka **Další.**
5. V průvodci **Opožděná nebo okamžitá žádost** vyberte **Okamžitě odeslat žádost certifikačnímu úřadu online** a klikněte na **Další.**
6. V názvu a nastavení zabezpečení zadejte do pole **Jméno** popisný název **Web-server CA** a pokračujte tlačítkem **Další.**
7. Vyplňte pole o**rganizace** a **organizační jednotka** jménem **Maxdat** a klepněte na **Další.**
8. V dialogovém okně **Běžný název webového serveru** ponechte **ca1** a stiskněte **Další.**
9. V **Zeměpisných informacích** zadejte l**ibovolné** hodnoty a opět stiskem tlačítka **Další** pokračujte v konfiguraci.
10. **Port SSL** ponechte na **výchozí** hodnotě a dejte **Další.**
11. U výběru certifikačního úřadu pokračujte tlačítkem **Další.**
12. V dialogovém okně **Odeslání žádosti o certifikát** si prohlédněte nastavení a pokud je vše v pořádku klepněte na tlačítko **Další** a následně na **Dokončit.**(viz obr.11)



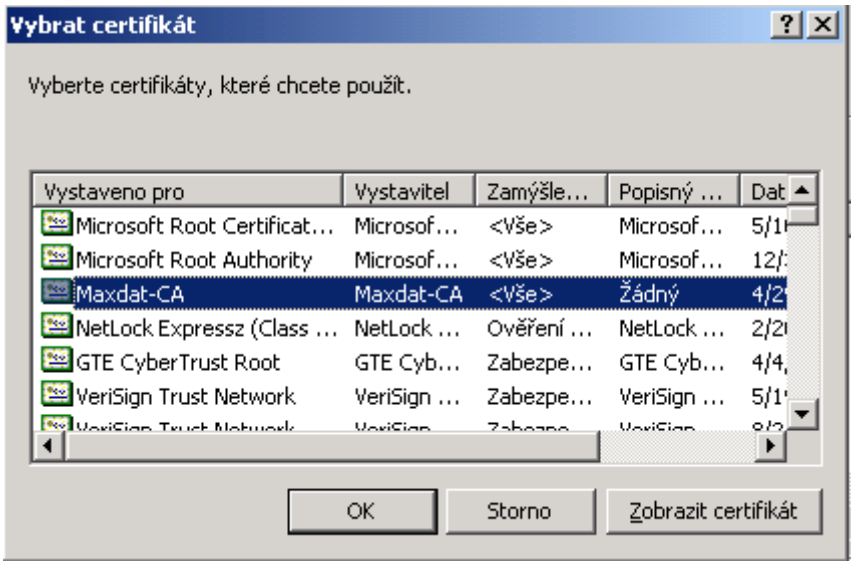
Obr. 11

13. Nyní v poli **Zabezpečená komunikace** stiskněte tlačítko **Upravit** a nastavte hodnoty tak jak je patrné na obrázku 12.



Obr. 12

14. Klikněte na tlačítko **Nový** a po zobrazení průvodce pokračujte stisknutím tlačítka **Další.**
15. V dialogovém okně **Certifikáty** v **seznamu CTL** klikněte na **Přidat z úložiště** a následně vyberte **certifikát Maxdat-CA** (viz obr.13) a stiskněte **OK.** Následně pokračujte tlačítkem **Další.**

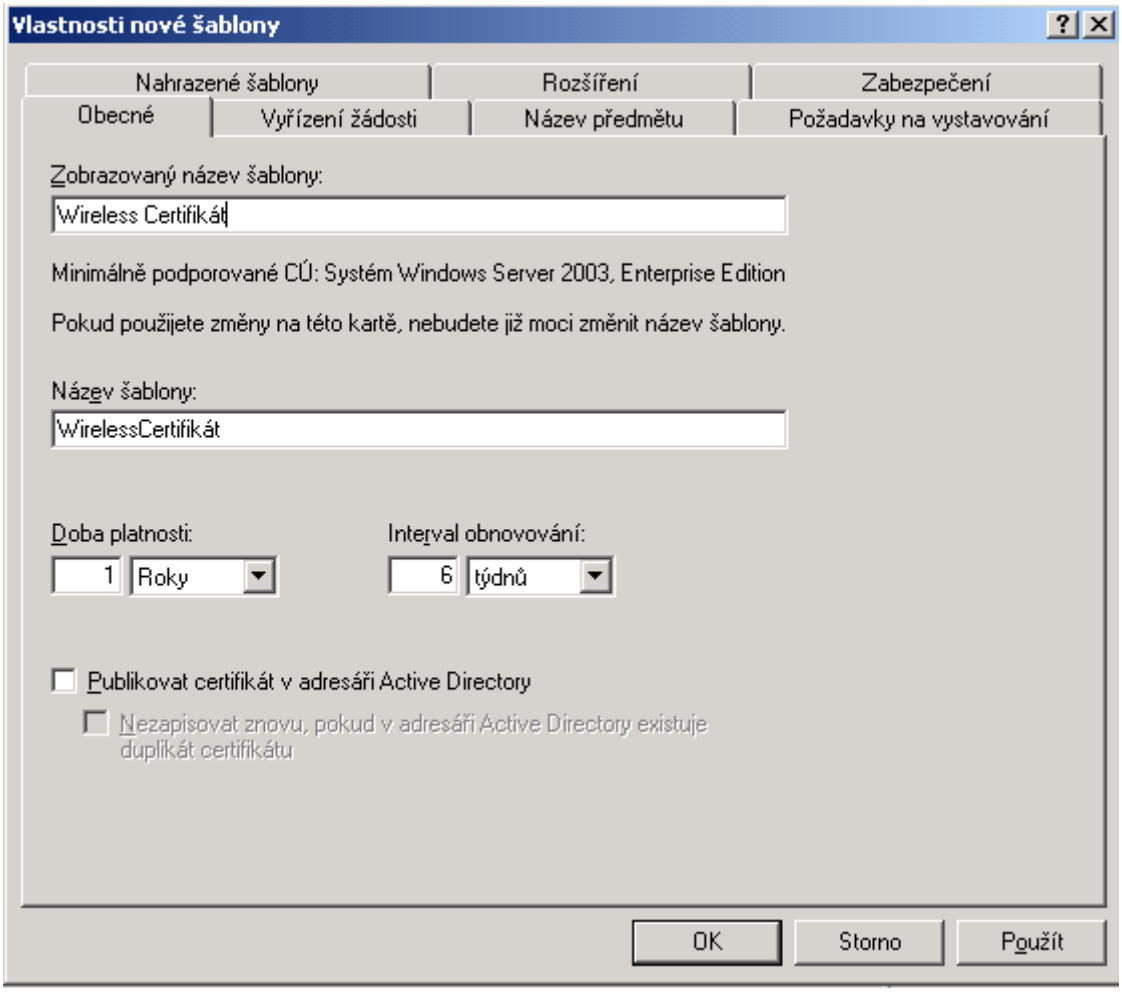


Obr. 13

16. V dialogovém okně **Název** a **popis** zadejte **IIScert** a klikněte na **Další.**
17. Konfiguraci dokončíte klepnutím na tlačítko **Dokončit.** Opusťte zbývající dialogová okna tlačítky **OK.**

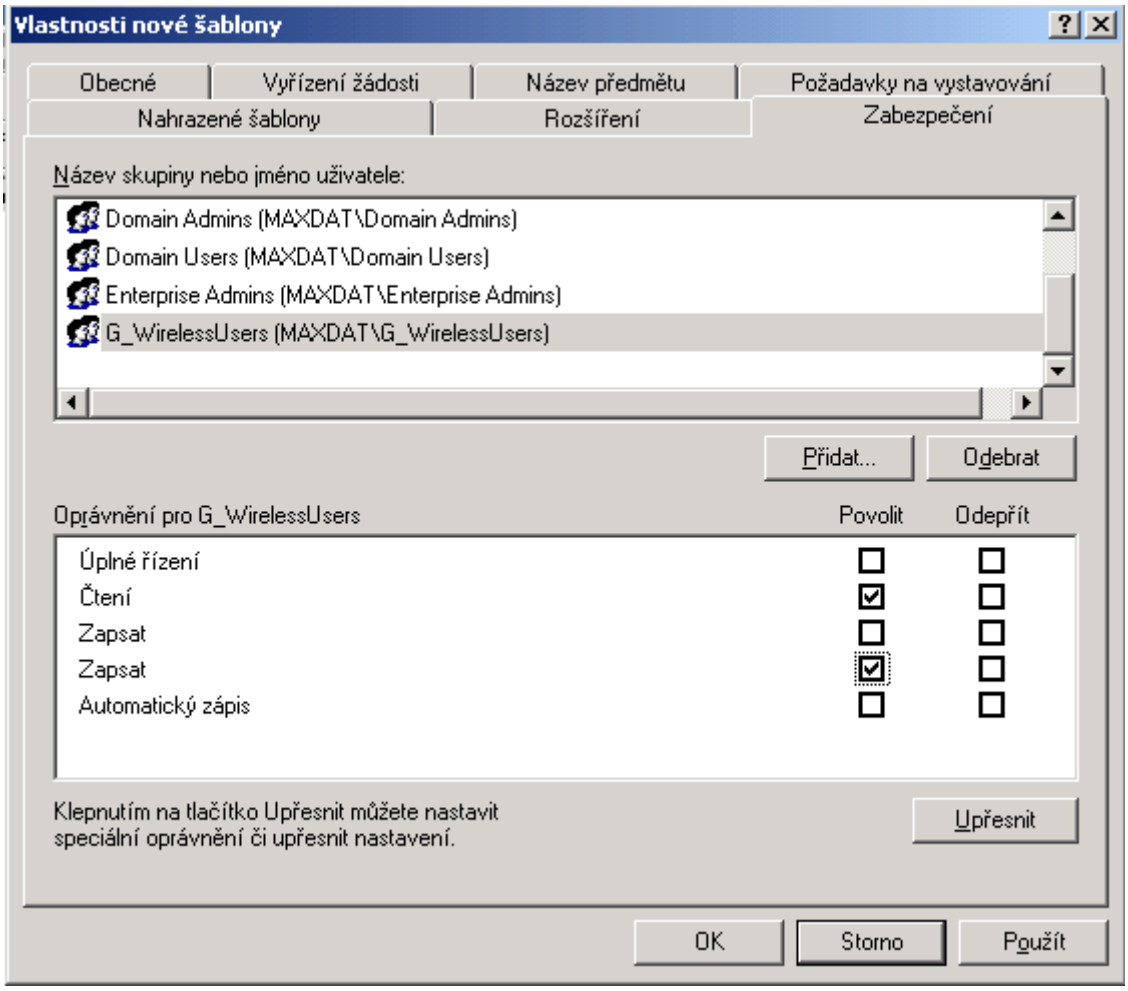
2.2.5. Vytvoření a publikování šablony certifikátu pro bezdrátové uživatele

1. Na serveru **CA1** najeďte do konzole **Certifikační úřad** a klepněte na soubor **Šablony certifikátů**. Klikněte na soubor **pravým** tlačítkem a zvolte **Spravovat.**
2. V **šabloně certifikátů** označte šablonu s názvem **Ověřená relace** pravým tlačítkem a vyberte **Vytvořit duplikát šablony**.[7] Zadejte popisný název šablony v poli **Zobrazovaný název šablony**, např. **Wireless Certifikát** jak je znázorněno na obr.14.



Obr. 14

3. Přejděte na kartu **Zabezpečení**, klikněte na tlačítko **Přidat** a v podokně **Zadejte názvy objektů** k výběru napište **G_WirelessUsers** a klepněte na **Kontrola názvů**.Potvrďte tlačítkem **OK.**
4. V okně **Zabezpečení** označte nově přidanou skupinu G_WirlessUsers a zaškrtněte ve sloupci **Povolit Čtení** a **Zapsat** jak ukazuje obrázek 15 a tlačítkem **OK** dokončete nastavení šablony.



Obr. 15

5. **Uzavřete** konzolu **Šablony certifikátů** a v konzole **Certifikačního úřadu** klikněte pravým tlačítkem na složku **Šablony certifikátů** a zvolte **Nová položka** -> **Vystavovaná šablona certifikátu.**
6. V dialogovém okně **Povolit šablony certifikátů** zvolte právě vytvořenou šablonu s názvem Wireless Certifikát a potvrďte **OK.**
7. **Uzavřete** konzolu a **odhlaste** se od serveru **CA1.**

3. IMPLEMENTACE ZABEZPEČENÍ 802.11i

3.1. Internet authentication server (Radius)

3.1.1. Instalace serveru Radius

1. Nainstalujte Windows server 2003 R2 Standard nebo Enterprise Edition na server (stand- alone)
2. Nastavte síťovou adresu TCP/IP protokolu na 192.168.20.4 a masku podsítě na 255.255.255.0, server DNS nastavte na 192.168.20.2.

3.1.2. Přidání serveru IAS do doménového prostředí

1. Najeďte do **Nabídky Start**, **pravým** tlačítkem klikněte na položku **Tento počítač** a zvolte **Vlastnosti**.
2. V dialogovém okně **Vlastnosti systému** zvolte kartu **Název počítače** a dejte **Změnit.**
3. V poli **název počítače** ověřte, že název je **ias.**
4. V poli **Je členem** vyberte volbu **Domény** a do jejího pole zadejte **maxdat.cz** a stiskněte **OK**.
5. **Zadejte** uživatelské jméno a heslo s oprávněním se připojit do domény (Administrator) a dejte **OK**.
6. Po zobrazení dialogového okna Vítejte v doméně maxdat.cz klikněte na **OK** a **OK** a po výzvě **restartujte** server.

3.1.3. Instalace služby Internet authentication services (radius)

1. **Přihlaste** se k serveru **Ias** jako **správce.**

2. V **Nabídce Start** přejděte na **Ovládací panely** a dále klikněte na **Přidat nebo odebrat programy.**[3]
3. V levém menu klikněte na **Přidat nebo odebrat součásti systému.**
4. **V průvodci součástmi** vyberte položku **Networking services** (síťové služby) a dále na **Podrobnosti.**
5. V okně **Networking services** zatrhněte položku **Internet authentication services** a klikněte na tlačítko **OK.** Po úspěšné instalaci klikněte na **Dokončit.**

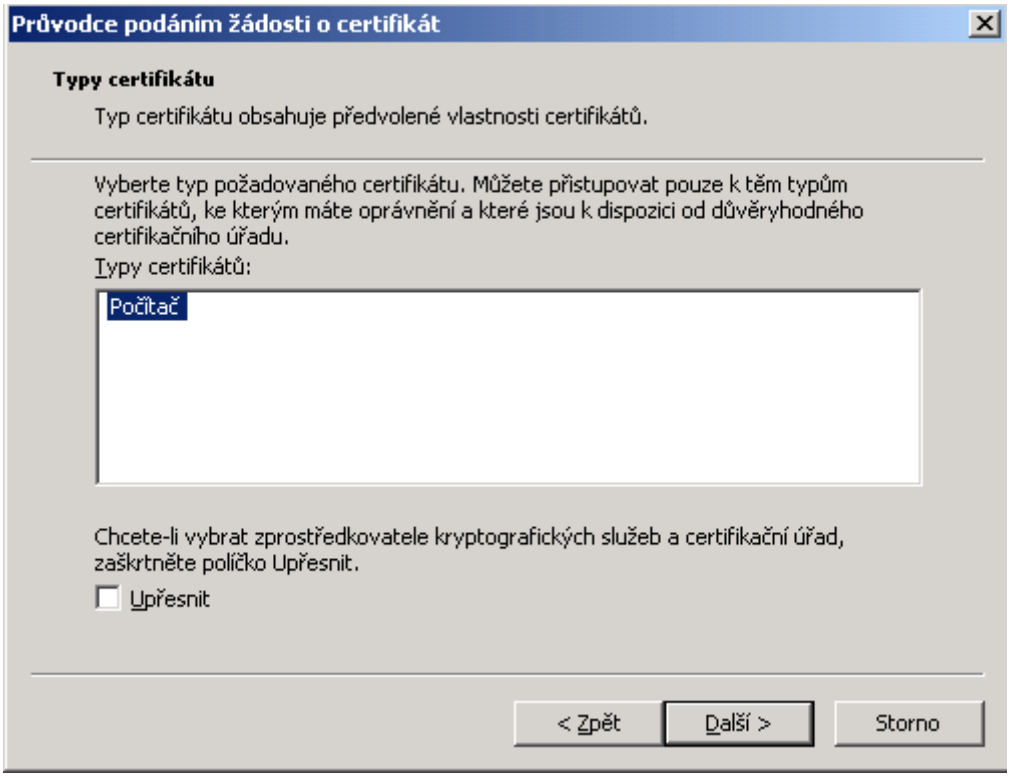
3.1.4. Konfigurace služby Internet authentication services (radius)

1. V **Nabídce Start** klikněte na **Nástroje pro správu** a vyberte **Služba ověřování v Internetu.**
2. V levém menu klikněte na položku **Internet Authentication service (local)** pravým tlačítkem a zvolte **Zaregistrovat server v adresáři Active Directory.**
3. Po zobrazení výstrah klepněte na tlačítko **OK.**

3.1.5. Vystavení ověřovacího certifikátu

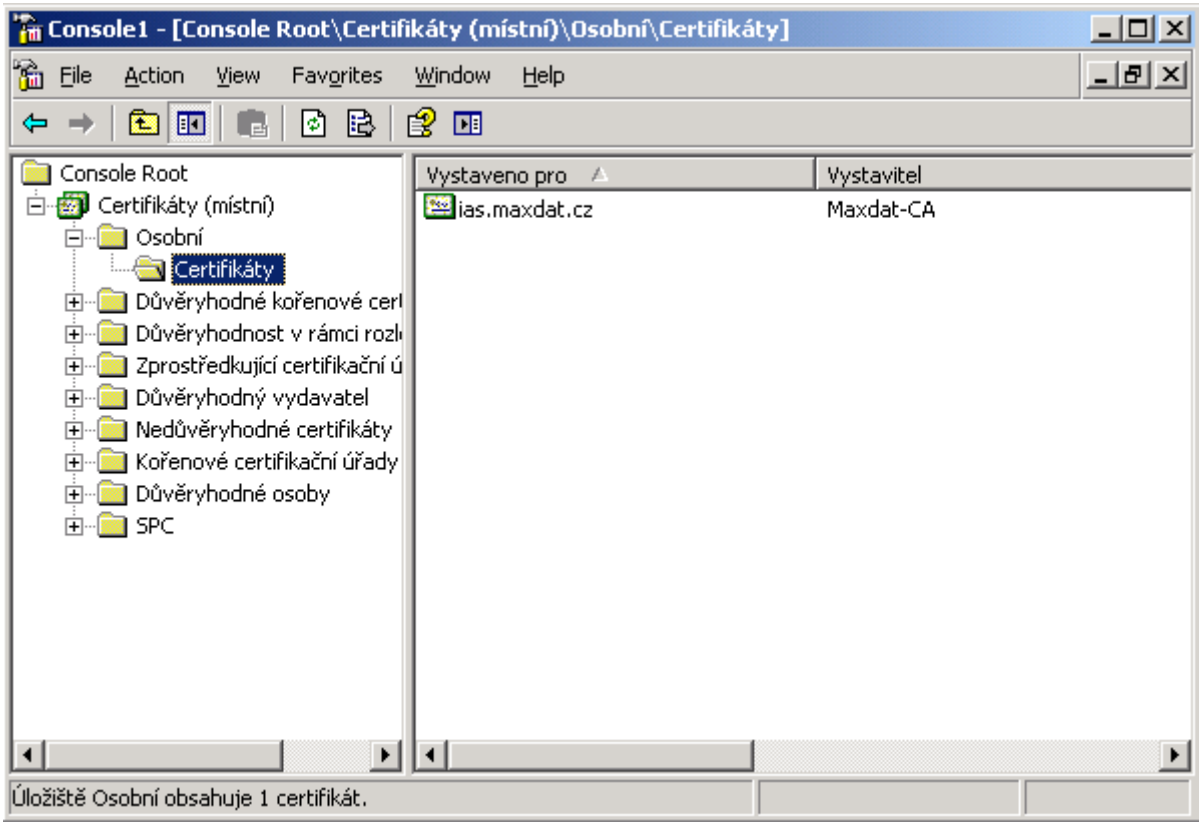
1. V **Nabídce Start** zvolte **Spustit** a do dialogového okna zadejte **mmc** a klikněte na **OK.**
2. Po otevření konzoly zvolte v menu **File - Add/Remove Snap- in** a v nově otevřeném dialogovém okně stiskněte tlačítko **Add.**
3. V okně **Add Standalone snapp-in** klikněte na **Certifikáty** a pokračujte stiskem tlačítka **Add.**
4. Po zobrazení dialogového okna **Modul snapp-in certifikáty** zvolte **Účet počítače** a stiskněte **Další.**
5. V sekci **Vybrat počítač** vyberte **Místní počítač (počítač, ve kterém je spuštěna tato konzola)** a klepněte na **Dokončit.**
6. **Opusťte** okno **snap-in** klepnutím na **Close** a **OK.**

7. Nyní v **okně mmc** rozbalte položku **Certifikáty** (**místní**), **pravým** tlačítkem klepněte na složku **Osobní**, vyberte **All Tasks** a následně **Požádat o nový certifikát.**
8. Po přečtení uvítacího průvodce klepněte na **Další.**
9. V dialogovém okně **Typy certifikátů** zvolte **Počítač** a pokračujte klepnutím na **Další.**(viz obr. 16)
10. v poli **Popisný název** zadejte **IAS certificate** a klepněte na **Další.**
11. Žádost o certifikát dokončíte stisknutím tlačítka **Dokončit.**



Obr. 16

Po kliknutí na složku **Osobní** - **Certifikáty** se Vám v pravém okně zobrazí nově vytvořený certifikát serveru, jak je znázorněno na obr. 17.

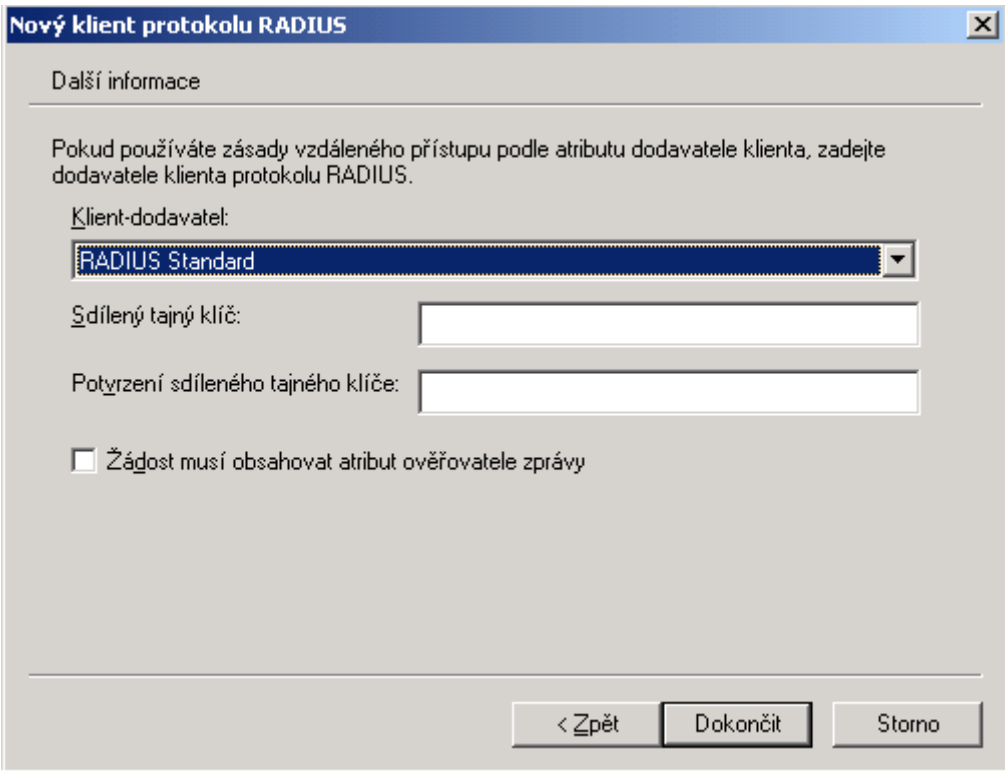


Obr. 17

3.1.6. Nastavení klienta Radius

1. V **Nabídce Start** - **Nástroje pro správu** klepněte na **Služba ověřování v Internetu.**[9]
2. V okně klikněte na **Klienti Radius** pravým tlačítkem a zvolte **Nový klient protokolu Radius.**
3. Do dialogového okna **Nový klient protokolu RADIUS** v poli **Popisný název** zadejte **AP1** a do pole **Adresa klienta (IP nebo DNS)** zadejte 192.168.20.5 a klikněte na **Další.**
4. V dalším dialogovém okně zvolte v poli **Klient-dodavatel** Radius Standard a pod ním zadejte **Sdílený tajný klíč** (viz obr. 18)**.** Po opětovném napsání sdíleného klíče klepněte na tlačítko **Dokončit.**

Pozn.: Sdílený tajný klíč budete opětovně zadávat při nastavování bezdrátového přístupového bodu.

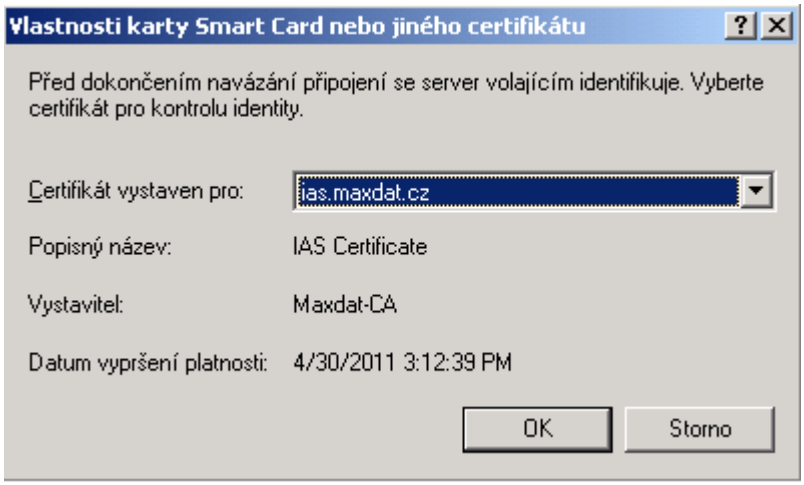


Obr. 18

3.1.7. Konfigurace zásad vzdáleného přístupu

1. Najeďte do konzoly **Služba ověřování v Internetu** a pravým tlačítkem klikněte na **Zásady vzdáleného přístupu**. Zvolte **Nové zásady vzdáleného přístupu** a pokračujte tlačítkem **Další.**
2. V dialogovém okně **Metoda konfigurace zásad** zvolte volbu **Použít průvodce k nastavení typické zásady v běžné situaci** a do pole **Název zásady** zadejte **Bezdrátový přístup** a pokračujte tlačítkem **Další.**
3. Na kartě **Metoda přístupu** označte volbu **Bezdrátový** a stiskněte **Další**.
4. V dialogovém okně **Přístup uživatele nebo skupiny** vyberte **Skupiny** a stiskněte **Přidat**.
5. Klikněte na **Umístění**, **označte** maxdat.cz a potvrďte tlačítkem **OK.**
6. **Do názvu objektů** zadejte G_WirelessUsers a stiskněte tlačítko **Kontrola názvů** pro ověření, zdali je název skupiny platný. Pokud ano, název se podtrhne a nastavení můžeme opustit tlačítkem **OK** a **Další**.

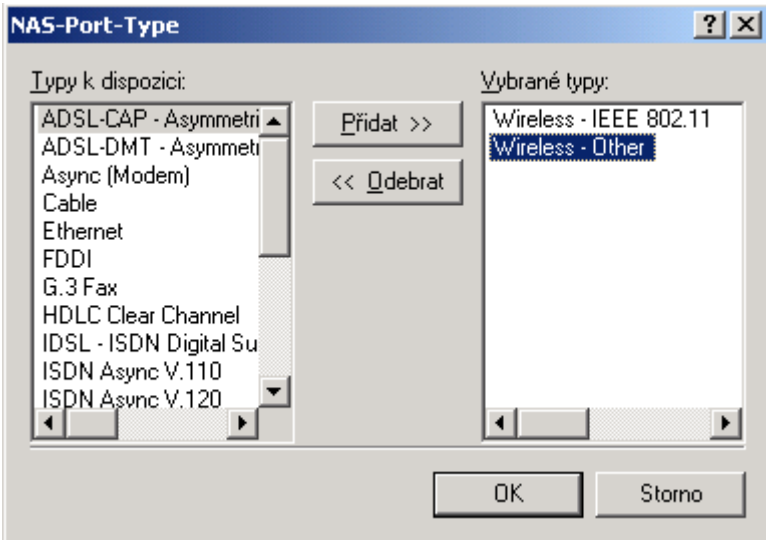
7. U **Metody ověřování** zvolíme **Smard Card or other certificate** a dále pokračujeme tlačítkem **Konfigurovat**. Ověříme, že v sekci **Certifikát vystaven pro** je **ias.maxdat.cz** (viz obr. 19) a dáme **OK** a **Další.**
8. Konfiguraci dokončíme tlačítkem **Dokončit**.



Obr. 19

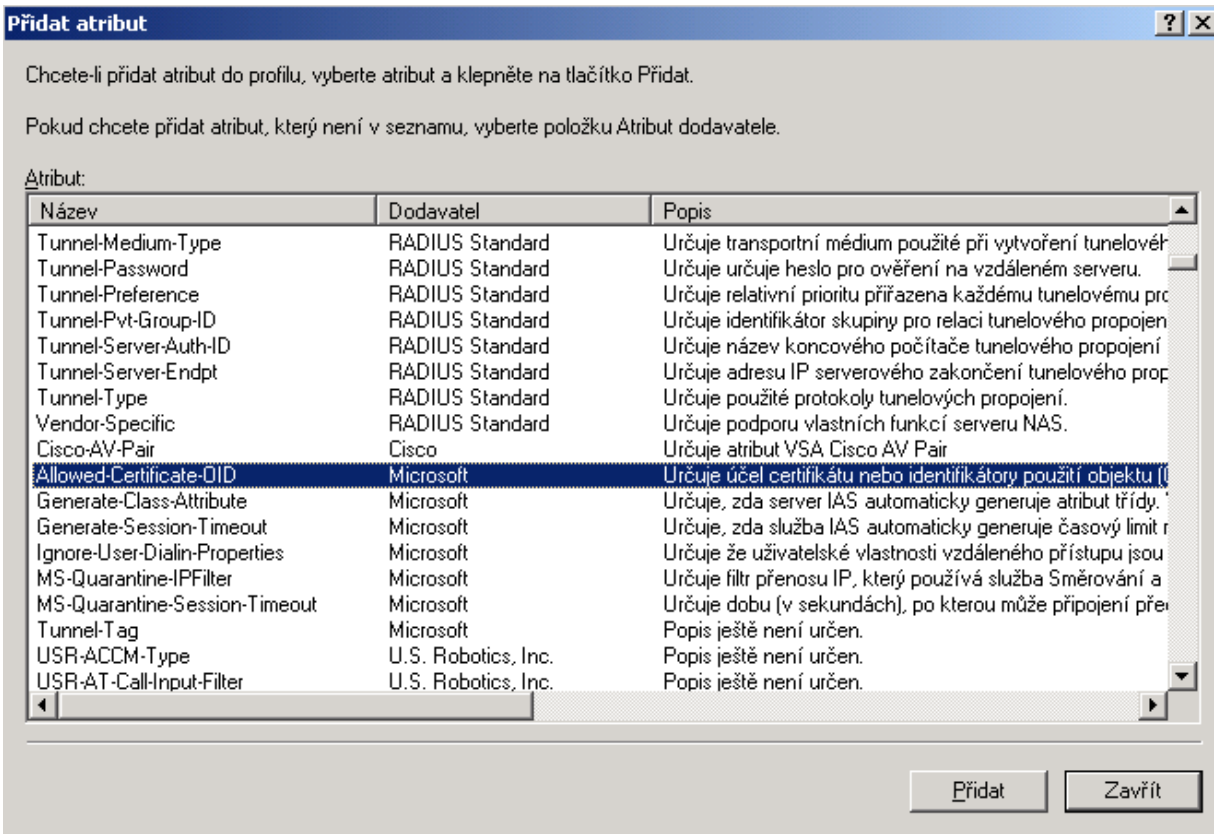
3.1.8. Posílení bezpečnosti EAP-TLS dle doporučení spol. Microsoft

1. V konzole **Služba ověřování v Internetu** klikněte na **Zásady vzdáleného přístupu.**
2. V pravém okně klikněte na položku **Bezdrátový přístup** pravým tlačítkem a zvolte **Vlastnosti (Properties).** [12]
3. Klikněte na **Upravit** a v dialogovém okně **NAS-Port-Type** označte v poli **Vybrané typy** položku **Wireless-Other** a klikněte na **Odebrat** (viz obr. 20). Potvrďte nastavení tlačítkem **OK.**



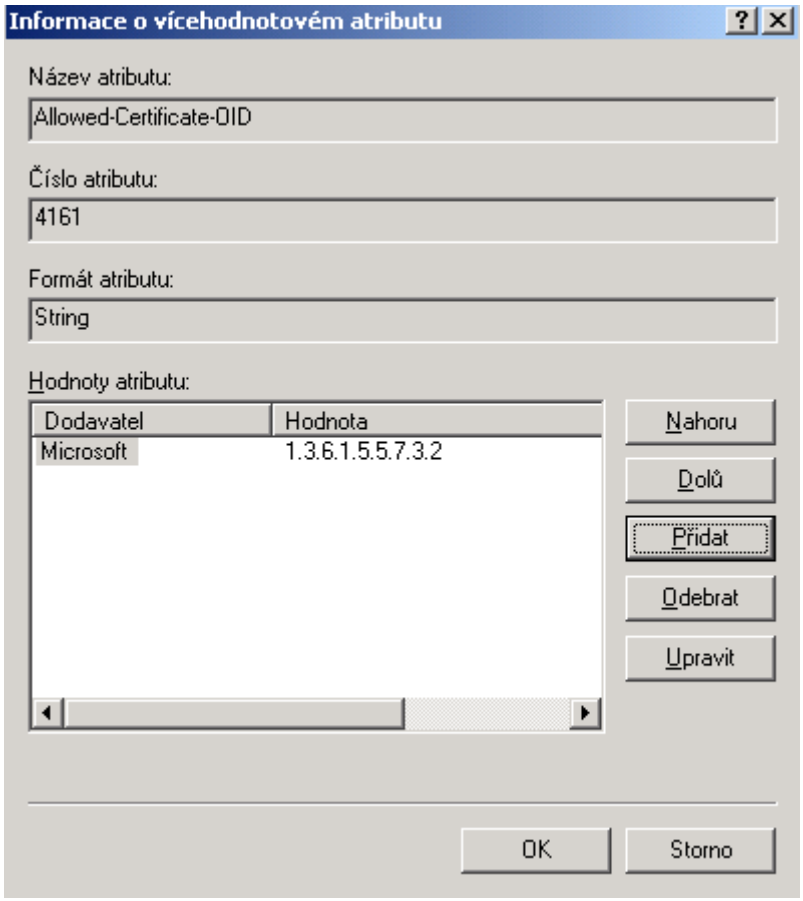
Obr. 20

4. Klikněte na **Upravit profil** a v dialogovém okně **Upravit profil telefonického připojení** klepněte na kartu **Upřesnit**. Stiskněte **Přidat** a následně v okně **Přidat atribut** vyhledejte v seznamu atribut s názvem **Allowed-Certificate-OID** jak je patrné na obrázku 21 a klikněte na **Přidat**.



Obr. 21

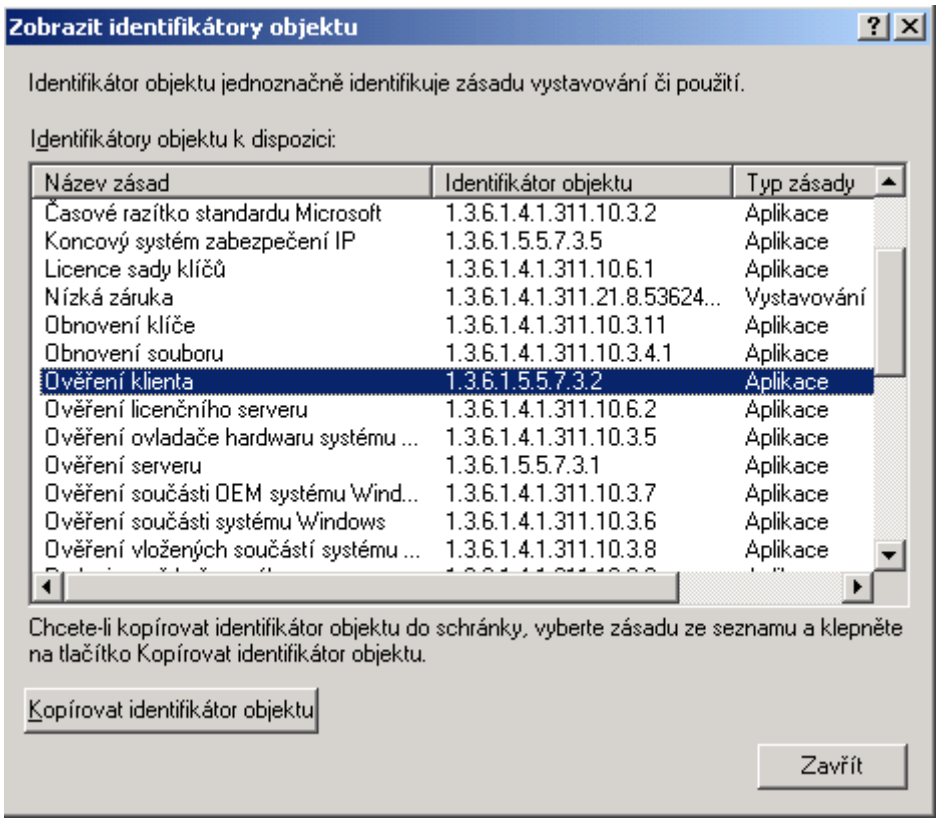
5. V okně **Informace o vícehodnotovém atributu** klikněte na tlačítko **Přidat** a do pole **Hodnoty atributu** zadejte řetězec **1.3.6.1.5.5.7.3.2** (obr. 22) Pokračujte stisknutím **OK.**



Obr. 22

6. Instalaci dokončíte stisknutím tlačítka **OK**-> **Zavřít**-> **OK** a **OK**.

Pozn.: OID odpovídá ověření klienta a hodnotu lze získat na serveru CA v konzole Certifikační úřad-> Šablony certifikátů v příkazu Zobrazit identifikátory objektu… (obr. 23)



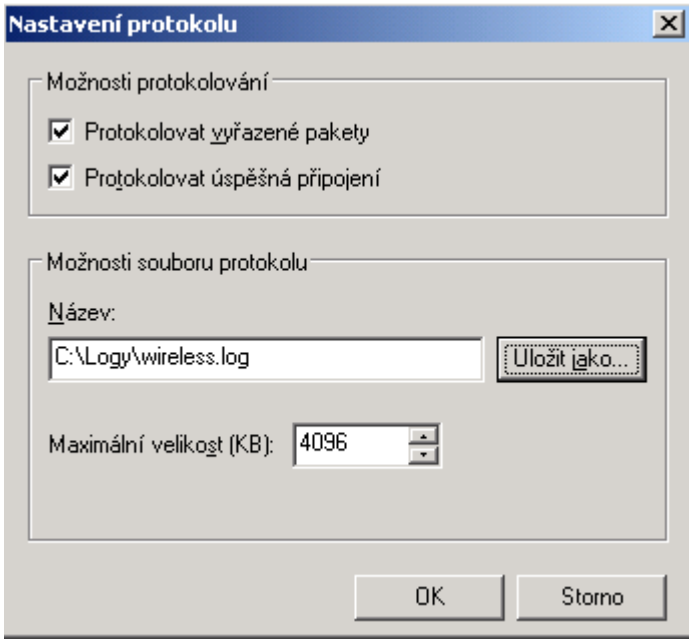
Obr. 23

3.1.9. Konfigurace firewallu a logování na radius serveru

1. Klikněte na **Nabídku Start** -> **Ovládací panely**->**Brána firewall systému Windows**.
2. Pokud se zobrazí okno požadující spuštění služby, stiskněte **Ano**.
3. Na kartě **Obecné** zvolte políčko **Zapnuto** a dále se přepněte na kartu **Výjimky**.
4. Stiskněte **Přidat port**, do pole **Název** zadejte **RADIUS Accounting** , v poli **Číslo portu** napište 1**812** a zvolte volbu **UDP**. Stiskněte **OK** pro potvrzení nastavení.
5. Stiskněte **Přidat port**, do pole **Název** zadejte **RADIUS Authentication** , v poli **Číslo portu** napište **1813** a zvolte volbu **UDP**. Následně stiskněte tlačítko **OK**.
6. Na kartě **Výjimky** ověřte, že jsou označené nově vytvořené služby a dále pokračujte na kartu **Upřesnit**.
7. V poli **Protokolování zabezpečení** stiskněte tlačítko **Nastavení** a v **Možnostech protokolování** zatrhněte volby **Protokolovat vyřazené pakety** a **Protokolovat úspěšná připojení**. V poli **Možnosti souboru protokolu** zadejte cestu, kde chcete

ukládat logy. V mém případě nastavím cestu na **C:\Logy\wireless.log** jak ukazuje obrázek 24. Pokračujte tlačítkem **OK**.

8. Celé nastavení dokončíte stisknutím tlačítka **OK**.



Obr. 24

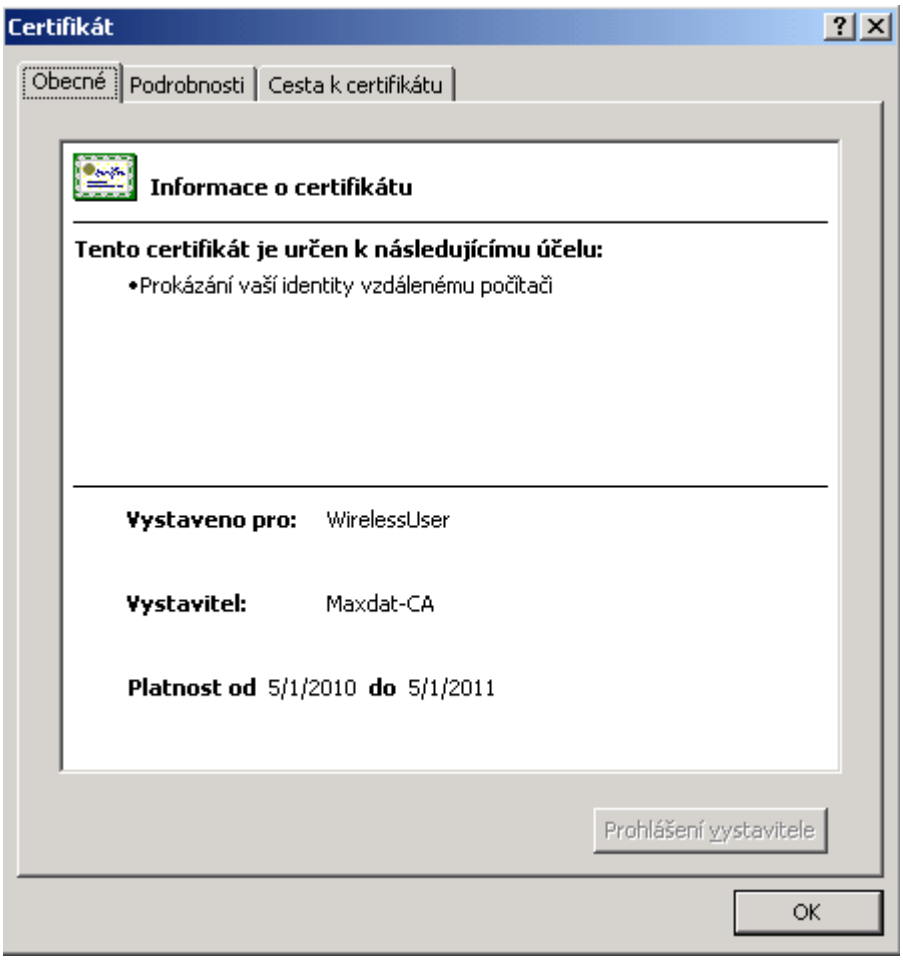
3.1.10. Vyžádání certifikátu klienta (WirelessUser)

1. **Přihlaste** se k serveru **CA1** jako **správce**.
2. **Spusťte** Internet Explorer a do pole adresa zadejte **https://ca1/certsrv** a dejte **Enter**.
3. Po zobrazení přihlašovacího dialogu zadejte uživatelské jméno. **maxdat.cz\WirelessUser** a heslo, které jste nastavili při konfiguraci uživatelského účtu.
4. **Přidejte** adresu do seznamu **povolených** adres a stiskněte **OK.**
5. Na webovém serveru v sekci **Select a task** klikněte na **Request a certificate**, dále na **Advanced Certificate Request** a pokračujte stisknutím volby **Create and submit a request to this CA.**
6. V dialogovém okně **Advanced Certificate Request** vyberte v poli **Certificate template** šablonu **Wireless Certifikát** a dole na stránce stiskněte **Submit**.

7. Po zobrazení výstrahy, že certifikát je žádán Vaším jménem, potvrďte tuto skutečnost tlačítkem **Ano** a dále stiskněte **OK**.
8. Nyní byl požadavek odeslán na CA, kde bude čekat na schválení.

Pozn.: V tomto případě jsme z důvodu jednoduchosti nastavili oprávnění Číst, Zapsat a Enroll skupině Administrators, ale v rozsáhlých produkčních prostředích je třeba pravomoci oddělit na další uživatele. V terminologii Microsoftu mluvíme o tzv. separaci rolí. Stejně žádosti o certifikát se obecně vytváří tak, že vybranému účtu přidělíme certifikát Enrollment agenta, který jako jediný má právo podepisovat certifikát naším jménem.

9. **Schválení /zamítnutí** požadavku na certifikát provedeme v konzole **Certifikační úřad** následujícím způsobem.
10. V konzole CA klikneme na složku **Žádosti čekající na vyřízení** a v pravém okně se Vám zobrazí řádek s hodinami.
11. Klikněte na řádek pravým tlačítkem a zvolte **Všechny úkoly** a následně **Vystavit**.
12. Nový certifikát se Vám přesunul do složky **Vystavené certifikáty** a je připravený k exportu.
13. Klikněte ve složce **Vystavené certifikáty** na řádek **Maxdat\WirelessUser** a zobrazí se Vám certifikát tak jak je znázorněno na obrázku 25.



Obr. 25

14. **Přejděte** na kartu **Podrobnosti** a zvolte **Kopírovat do souboru**. Po přečtení průvodce stiskněte **Další**.
15. V dialogovém okně **Formát souboru pro export**, zvolte **Binární X. 509**, **kódování DER (*.cer)** a stiskněte **Další**.
16. V **Souboru pro export** zadejte umístění např. na **plochu**, pojmenujte certifikát **WirelessUser** a pokračujte tlačítkem **Uložit**.
17. Export certifikátu dokončíte tlačítkem **Další** a **Dokončit**.
18. **Vystavení certifikátu CA a CRL** provedeme z **webové konzoly**.
19. **Spusťte** Internet Explorer a do pole adresa zadejte **https://ca1/certsrv** a stiskněte **Enter**.
20. Po zobrazení přihlašovacího dialogu zadejte uživatelské jméno **maxdat.cz\WirelessUser** a **heslo**.
21. V sekci **Select a task** klikněte na **Download a CA certificate, certificate chain, or CRL.**

22. Stiskněte **Download CA certificate chain**, pojmenujte ho **Kotva** a **uložte** soubor **na Plochu**.
23. **Oba** soubory si uložte na **USB disk** a **odhlaste** se od serveru.

3.1.11. Nastavení bezdrátového přístupového bodu

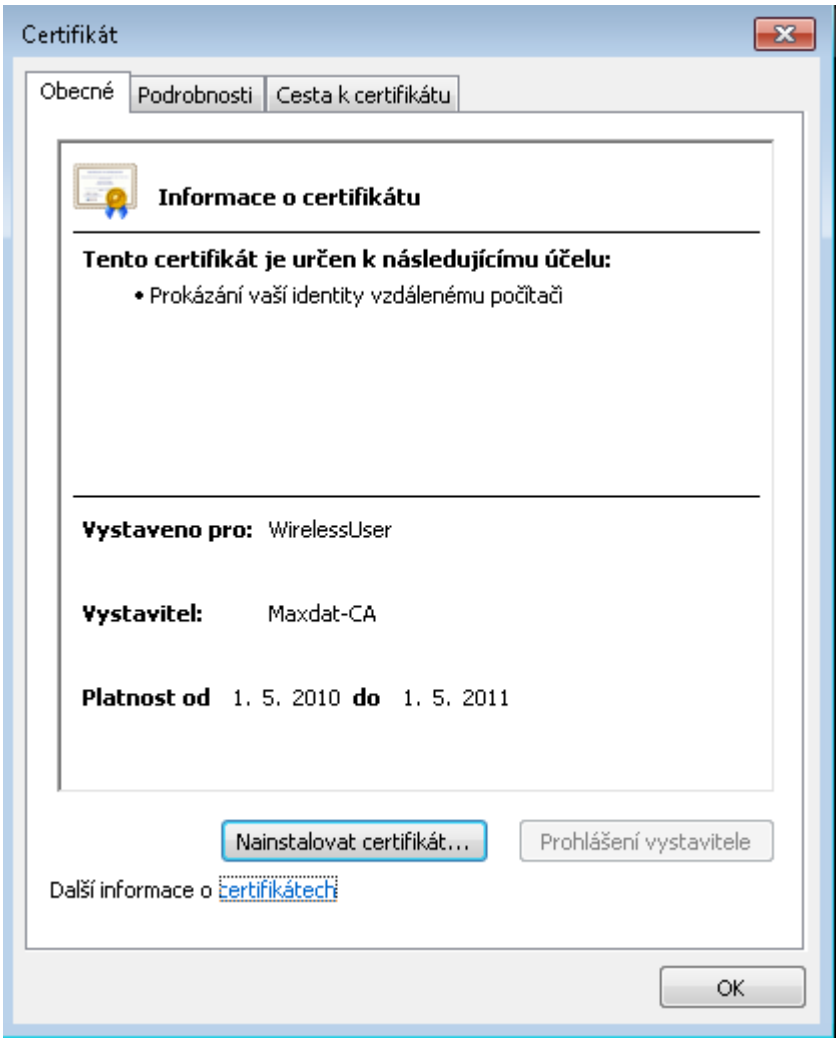
1. Nastavte AP **IP adresu** na 192.168.20.5, **maska podsítě** 255.255.255.0, **DNS** 192.168.20.2.
2. Zvolte zabezpečení typu **WPA2-enterprise**, kódování **AES**.
3. **SSID** Maxdat.
4. Zadejte **Radius předsdílený tajný klíč** (klíč , který jsme nastavili při konfiguraci IAS radius).

Pozn.: Zadané informace jsou obecné, protože nastavení AP se liší v závislosti na tom, od jaké společnosti AP pochází.

4. ZABEZPEČENÍ KLIENTSKÝCH STANIC

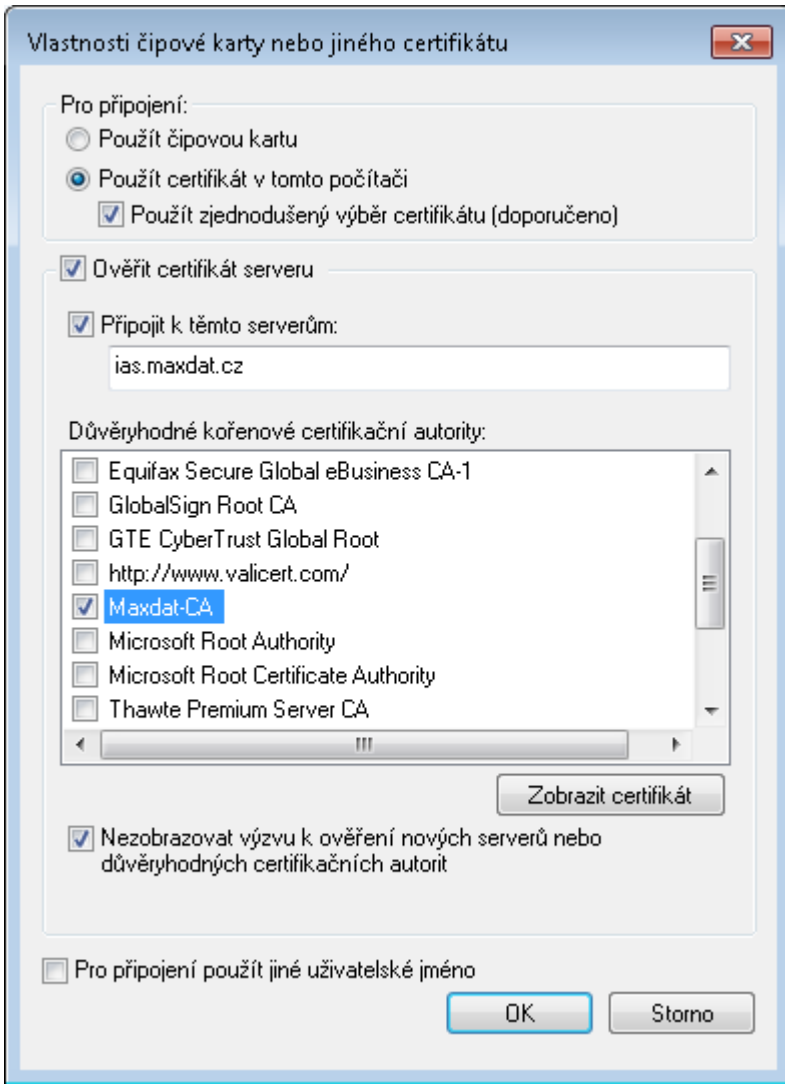
4.1.Nastavení zabezpečené komunikace pracovních stanic

1. **Nainstalujte** Windows 7 na klientskou stanici.
2. **Vložte** USB disk s certifikáty do pc a po zobrazení **klikněte** na certifikát s názvem **Kotva** pravým tlačítkem a vyberte **Nainstalovat certifikát**.
3. Po zobrazení průvodce Průvodcem certifikátu stiskněte **Další**.
4. V dialogovém okně **Úložiště certifikátů** vyberte **Všechny certifikáty umístit v následujícím úložišti** a klepněte na **Procházet**.
5. V okně **Vybrat úložiště certifikátů** označte složku **Důvěryhodné kořenové certifikační autority** a potvrďte výběr tlačítkem **OK**. Následně pokračujte tlačítkem **Další** a **Dokončit**.
6. Po zobrazení upozornění, zdali skutečně chcete nainstalovat certifikát CA, klikněte na **Ano**.
7. Nyní poklepejte na druhý certifikát označený **WirelessUser**. Na kartě **Obecné** stiskněte **Nainstalovat certifikát** (vizobr.26). Opět se zobrazí průvodce importem certifikátu.Pokračujte tlačítkem **Další**.



Obr. 26

8. V dialogovém okně **Úložiště certifikátů** vyberte **Všechny certifikáty umístit v následujícím úložišti** a klepněte na **Procházet**.
9. Vyberte složku **Osobní** a stiskněte **OK**. Průvodce dokončíte tlačítky **Další**, **Dokončit** a **OK**.
10. **Přejděte** do **Nabídky Start**, **Ovládací panely** -> **Síť a Internet** ->**Centrum síťových připojení a sdílení** a v levém menu klikněte na **Spravovat bezdrátové sítě**.
11. Zvolte **Přidat** a v dialogovém okně vyberte **Ručně vytvořit síťový profil**.
12. Zadejte **název sítě**, který jste nastavili u AP**, typ zabezpečení** zvolte **WPA2-podnikové**, **typ šifrování AES** a zatrhněte volbu **Vytvořit připojení automaticky**. Stiskněte **Další**.
13. Stiskněte **Změnit nastavení připojení**, přejděte na kartu **Zabezpečení** a v poli **Zvolte metodu ověřování v síti** vyberte **Microsoft:Čipová karta nebo jiný certifikát** a klikněte na **nastavení**. Proveďte nastavení jednotlivých voleb jak ukazuje obrázek 27.



Obr. 27

14. **Potvrďte** nastavení tlačítkem **OK** a přejděte na tlačítko **Upřesnit nastavení**.
15. Na kartě **Nastavení protokolu 802.1X** zatrhněte políčko **Zadejte režim ověřování** a v jeho záložce vyberte **Ověření uživatele**. Ostatní položky nechejte ve **výchozím** nastavení a opusťte nastavení tlačítky OK.
16. Nyní dojde k autentizaci.
17. Úspěšné nastavení můžete ověřit vložením adresy https://ca1/certsrv do Internet Exploreru na klientské stanici., kdy se Vám zobrazí webové rozhraní CA1.

Závěr

Je potřeba říci, že tato nastavení jsou velmi obecná a v praxi se konfigurace může lišit. Pro rozsáhlá produkční prostředí je potřeba dodělat mnohé další nastavení. Zejména nakonfigurování sekundárního IAS serveru, který bude řešit výpadek hlavního serveru nebo nastavení forwarderu DNS a výchozí brány (gateway), aby provoz byl směrován například do internetu. Co se týče infrastruktury PKI, při užití v produkčním prostředí Vás překvapí množství nedotažených věcí. Některé z nich lze díky dobré dokumentaci doprogramovat nebo je lze zakoupit od třetích stran. Zejména se zmíním o záloze CA a obnovení po havárii, což je nejkritičtějším bodem celé infrastruktury vůbec. Samotná CA nabízí standardní zálohování, ale před havárií mohou být vydány certifikáty, které nejsou ještě v poslední záloze.

Řešením je tzv. Exit modul, který bude zachytávat jednotlivé akce a ukládat je na SQL server. Dalším problémem CA je, že není full tolerant, tzn. nepodporuje cluster. Poslední záležitostí je samotná administrace certifikátů. Přes webové rozhraní certifikáty klientům sice lze vydat,ale už je neodvoláme. Přes mmc konzolu lze tyto úkony sice provádět, ale myšlenka, že by úřednice používala tento nástroj, je přinejmenším úsměvná. Na druhou stranu, kvůli astronomickým cenám komerčních produktů jako je třeba RSA Keon CA, Baltimore CA nebo Entrust CA je Microsoft CA docela vhodným řešením a navíc je “zdarma”.

Seznam použité literatury

[1]. **Hurley, Chris.** *How to cheat at Securing a Wireless Network.* Rockland : Syngress, 2006. 1597490873.

[2]. **Mc Clure, Stuart.** *Hacking bez tajemství, 3.aktualizované vydání.* Brno : Computer Press, 2003. 80-7226-948-8.

[3]. **Kwan, Philip.** *White paper: 802.1X port authentication with Microsoft´s active directory.* San Jose : Foundry Networks, 2003. e-book.

[4]. **Morimoto, Rand.** *Microsoft Windows Server 2003 Unleashed, R2 Edition.* Indianapolis : Sams Publishing , 2006. 0-672-32898-4.

[5]. **Barken, Lee.** *Jak zabezpečit bezdrátovou síť Wi-FI.* Brno : Computer Press , 2004. 80-251-0346-3.

[6]. **Šetka, Petr.** *Mistrovství v Windows server 2003.* Brno : Computer Press, 2003. 80-251-0036-7.

[7]. **Team, Microsoft Network.** *Windows Server 2008 Networking and Network Access Protection (NAP).* Redmond : Microsoft Press, 2008. 0-7356-2422-4.

[8]. **Komar, Brian.** *Windows Server 2008 PKI and Certificate Security.* Redmond : Microsoft Press, 2008. 0-7356-2516-6.

[9]. **E.Earle, Aron.** *Wireless Security Handbook.* Boca Raton : Auerbach Publications , 2006. 0-8493-3378-4.

[10]. **Schinder, Thomas.** *ISA server 2000.* Brno : Computer Press, 2003. 80-7226-916-X.

[11]. **Malina, Patrik.** *Windows Server 2003 Hotová řešení.* Brno : Computer Press, 2006. 80-251-1096-6.

[12]. **Smith, Ben, Komar, Brian.** *Zabezpečení systému a sítě.* Brno : Computer Press, 2006. 80-251-1260-8.

[13]. **Henrickson, Hethe.** *IIS6 Kompletní průvodce.* Brno : Computer Press, 2004. 80-251-0128-2.

[14]. **Dostálek, Libor, Vohnoutová, Marta.** *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* Brno : Computer Press, 2007. 80-251-0828-7.

Internetové odkazy

http://www.wlana.org/learning_center.html

http://aboba.drizzlehosting.com/IEEE/

http://www.cs.umd.edu/~waa/1x.pdf

http://grouper.ieee.org/groups/802/11/index.html

http://standards.ieee.org/getieee802/index.html

http://www.drizzle.com/